О.Є. Гудзь
А.А. Захаржевська

УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ

О.Є. Гудзь
А.А. Захаржевська

УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ

Навчальний посібник

Кропивницький
Видавець Лисенко В.Ф.
2023

УДК 621.391:004.056.54(075.8)
Г 93

Рекомендовано до друку Вченою радою Державного університету телекомунікацій (протокол № 16 від 10.05.2023 р.).

Рецензенти:

Боняр С. М. доктор економічних наук, професор;
Зеліско І.М. доктор економічних наук, професор;
Прокопенко Н.С. доктор економічних наук, професор.

Укладачі:

Гудзь Олена Євгенівна, доктор економічних наук, професор;
Захаржевська Аліна Анатоліївна, кандидат економічних наук.

Гудзь О.Є., Захаржевська А.А.

Г 93 Управління ризиками підприємств в умовах цифровізації: навчальний посібник. – Кропивницький : Видавець Лисенко В. Ф., 2023. – 176 с.

ISBN 978-617-7813-79-7

У навчальному посібнику розкрито основні поняття й терміни управління ризиками підприємств в умовах цифровізації та висвітлено теоретико-методологічні, аналітичні, прогностичні і прагматичні питання щодо управління ризиками підприємств в умовах цифровізації, що сприятиме формуванню системи знань у галузі управління ризиками, механізмів, діагностики та інструментарію прийняття рішень, отриманню глибоких уявлень стосовно порівняльних характеристик та пріоритетних напрямів розвитку й удосконаленню управління ризиками підприємств в умовах цифровізації, навичок самостійного творчого мислення, прийняттю оптимальних управлінських рішень, що забезпечить перехід до нової якості функціонування підприємств та стимулюватиме підвищення їх результативності, адаптивності, зрілості й гнучкості.

Рекомендовано для викладачів, аспірантів, здобувачів вищої освіти економічних спеціальностей, керівників й працівників державних установ та підприємств. Матеріали посібника будуть також корисними всім, хто цікавиться теоретико-методологічними й практичними аспектами управління ризиками підприємств в умовах цифровізації.

УДК 621.391:004.056.54(075.8)

ISBN 978-617-7813-79-7

ЗМІСТ

ПЕРЕДМОВА

Стрімке зростання кількості збиткових та неплатоспроможних підприємств спричинили кризові деформації економічного простору України, зумовлені введенням жорсткого локдауну, спровокованого пандемією COVID-19, а потім запровадженням воєнного стану, як реакції на повномасштабну збройну агресію Російської Федерації проти України. Для того, щоб вистояти у ці непрості часи, підприємства ведуть пошук і опрацьовують нові стратегії, технології, інструменти, методи управління ризиками. Проте, вітчизняні реалії сьогодення унеможливлюють це завдання, оскільки, більшість підприємств в умовах цифровізації, опирається на застарілу фрагментарну парадигму розвитку управління ризиками. Тому, формування нової філософії управління ризиками підприємств в умовах цифровізації що передбачає необхідність докорінних якісних перетворень, перехід від невизначеності до зрілості, організаційної різноманітності й гнучкості, зміни пріоритетів і цінностей, набуває вагомого значення та актуалізується.

У навчальному посібнику розкрито основні поняття й терміни управління ризиками підприємств в умовах цифровізації та висвітлено теоретико-методологічні, аналітичні, прогностичні і прагматичні питання щодо управління ризиками підприємств в умовах цифровізації, що сприятиме формуванню системи знань у галузі управління ризиками, механізмів, діагностики та інструментарію прийняття рішень, отриманню глибоких уявлень стосовно порівняльних характеристик та пріоритетних напрямів розвитку й удосконаленню управління ризиками підприємств в умовах цифровізації, навичок самостійного творчого мислення, прийняттю оптимальних управлінських рішень, що забезпечить перехід до нової якості функціонування підприємств та стимулюватиме підвищення їх результативності, адаптивності, зрілості й гнучкості.

Текст навчального посібника доповнюється статистичними даними і посиланнями на вітчизняні та іноземні бібліографічні джерела.

Автори висловлюють щиру подяку професору В.Б. Толубко, професору Л.Н. Беркман та рецензентам монографії професорам Ботвиній Н.О., Гривківській О.В., Лазоренко Л.В. чиї поради для підготовки навчального посібника є безцінними.

Видання пропонується для викладачів, аспірантів, здобувачів вищої освіти економічних спеціальностей, керівників й працівників державних установ та підприємств та буде корисним усім, хто цікавиться теоретико-методологічними й практичними аспектами управління ризиками підприємств в умовах цифровізації.

МОДУЛЬ 1
ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ

1.1. Сутнісна характеристика управління ризиками підприємств

Проблема управління ризиками підприємств вважається досить актуальною у теоретичному та практичному зрізі. Брак фінансових ресурсів, обмеженість впровадження інновацій і відсутність адекватних стратегій робить цей процес недореалізованим, що посилюється наявністю зношеної матеріально-технічної бази, застарілого технологічного обладнання, недостатністю компетентного персоналу, дефіцитом результативних механізмів управління ризиками підприємств та недосконалістю понятійного апарату. Цікаво, що наявність потужного наукового базису із різноманітністю наукових підходів щодо визначення сутності понять „ризик", „управління", залишає означену проблематику дискусійною. Тому, варто більш детально розглянути сутність та змістове наповнення даних понять, окреслити їх ключові переваги й обмеження, виявити характеристики, конститутивні атрибути та властивості процесу управління ризиками підприємств.

Діяльність усіх підприємств тісно переплітається з ризиками. „У процесі своєї діяльності підприємства стикаються з різними видами ризиків, які розрізняються між собою місцем і часом виникнення, сукупністю зовнішніх і внутрішніх чинників, що впливають на їх параметри, способом їх аналізу і методами впливу" [31].

Поняття „ризик" у загальному визначені бере свій родовід від давньогрецького „ridsicon", що означає скеля чи небезпека зіткнення з нею; древньою італійською „risicare", що перекладається, як „посміти", „наважитися"; французького слова – „risdoe", що трактується, як загроза чи йти на ризик. І. А. Бланк обґрунтовує, що „поняття „ризик" має доволі давню етимологію, що бере свій початок від первіснообщинного ладу, зокрема, первісні люди, граючи в азартні ігри, оцінювали свої ризики" [11 с.10]. З розвитком суспільних відносин генеруються різні тлумачення ризику, поглиблюється їх зміст та розширюються сфери застосування. Еволюцію поняття „ризик" продемонстровано у додатку А. Проте, переважно, дослідники, походження ризику пов'язували „із загальнонауковими дисциплінами: філософією та економікою" [190].

Адам Сміт (1723 – 1790 рр.) у своєму видатному творі „Дослідження про природу і причини багатства народів", стверджував, що „ризик є чинником частки прибутку, оскільки досягнення, навіть, звичайної норми прибутку пов'язане з більшим чи меншим ризиком" [188]. Водночас, Йоганн фон Тюнен (1783 – 1850 рр.) акцентував „на відмінностях між ризиком, який можна застрахувати і ризиком, що не може бути застрахованим – йому повинна відповідати частка прибутку, яка розглядається як плата за можливість банкрутства" [188]. Далі, термін „ризик" з початку XX ст. активно

використовується у багатьох практичних галузях та наукових розвідках. Так, „ризик" від окремих точних наук (механіка, математика, статистика, фізика) розповсюджується на гуманітарні наукові дослідження – економіки, психології, біології, демографії, права тощо. Дослідження Ф. Найта, Д. Робертсона, Дж. М. Кейнса, Дж. Мілля, А. Маршала, А. Пігу та інших вчених, мали вирішальний вплив на поступ теорії ризиків. „Поняття ризику було пов'язано з можливим виникненням втрат, недоодержанням доходу або прибутку" [139]. Практично, у цей період формуються дві основні теоретичні течії (класична і неокласична) щодо пояснення природи економічного ризику. Фундаторами класичної течії, вважають Дж. Мілля та Н. У. Сеніора, які доводили, що підприємницький дохід складається з частки від інвестованого капіталу, заробітної плати підприємця та компенсації за підприємницький ризик.

Тобто, ризик, вони розглядали як математичний розрахунок можливих втрат, які підприємець може понести внаслідок реалізації ухваленого рішення. Таким чином, класична теорія ризику, трактує його як ймовірність отримання збитків від обраної стратегії діяльності. Фундаторами неокласичної течії, вважають видатних науковців А. Маршалла та А. Пігу, які доводили, що „підприємництво в умовах невизначеності має керуватися двома категоріями: розміром очікуваного прибутку та величиною можливих втрат" [190]. Американський дослідник Ф. Найт, який в 1921 р. першим запропонував розмежувати категорії „невизначеність" і „ризик", акцентував увагу на „принциповій вимірності останнього, відтінюючи його як „вимірну невизначеність" [51]. Видатний англійський дослідник Дж. М. Кейнс окреслює „невизначеність як наслідок ірраціональностей, притаманних природі людини", і далі доходить висновку, що „слід обов'язково враховувати діяльність людини як джерело невизначеності, а відтак і ймовірних втрат та враховувати притаманну людині схильність до ризику" [188].

На підставі великої чисельності трактувань різних дослідників (додаток), можемо стверджувати, що ризик – це багатогранне й складне поняття.

Цікаво, що колектив вчених під провідом А. В. Руснака обґрунтовує, що „ризик це діяльність суб'єктів підприємницької діяльності, що пов'язана з подоланням невизначеності в ситуації неминучого вибору, у процесі якої є можливість оцінити вірогідність досягнення бажаного результату, невдачі, відхилення від мети, що містяться у вірогідних альтернативах"[152].

За переконанням О. Б. Секеріна: „ризик − це характеристика підприємницької діяльності, пов'язана із суб'єктивною оцінкою підприємством наслідків впливу чинників невизначеності на результати рішення, що приймається з точки зору сприятливого і несприятливого впливу" [145 с. 69]. Акцентуємо, що ризику притаманне „діалектичне об'єктивно-суб'єктивне" [23] змістове наповнення (рис. 1.1).

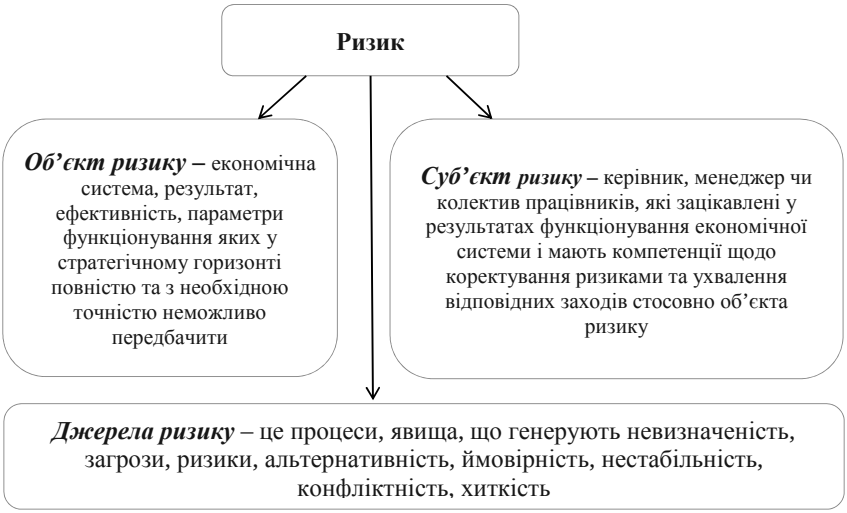


Рис. 1.1. Діалектичне об'єктивно-суб'єктивне змістове наповнення ризику
Примітка: сформовано на основі [23].

Рисунок 1.1. наочно демонструє помітний взаємозв'язок „ризику" з термінами ймовірності й невизначеності. Звертаємо увагу, що чинник ймовірності, невизначеності, відчутно впливає на ефекти ризику, які виражаються у негативному, позитивному чи нейтральному форматі (рис. 1.2).

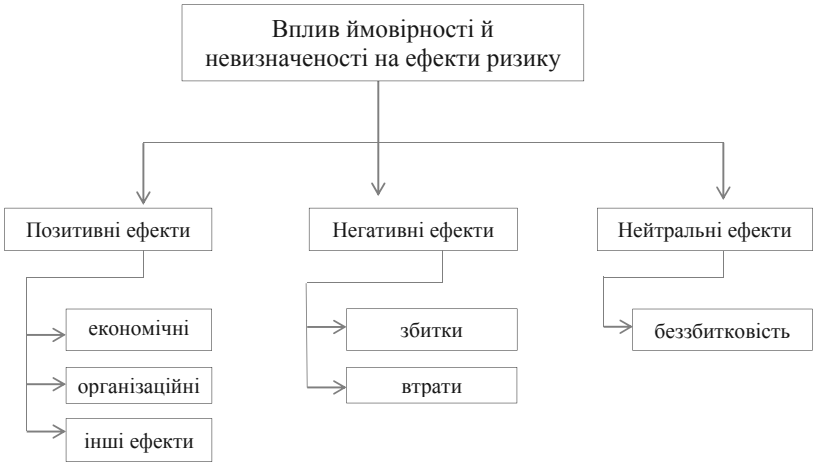


Рис. 1.2. Вплив ймовірності й невизначеності на ефекти ризику
Примітка: сформовано на основі [167 с. 124].

„Ймовірність” (від латинської „probabilitas” чи англійської „probability”) – це окреслення можливості того, що певна випадкова подія здійсниться за умов, які можуть багато чисельно повторюватися. А, наявність невизначеності пояснюється дослідниками як „передумова виникнення ризику, фундаментальна характеристика недостатньої забезпеченості процесу прийняття економічних рішень знаннями стосовно певної проблемної ситуації” [171 с. 16]. Водночас, передумовами ризику вважаються ще й конфліктність, альтернативність та хиткість.

Розгляд різноманітних наукових публікацій дає змогу, стверджувати, що, багато вчених розглядають ризик „post factum”, тобто не здійснюючи його превентивної оцінки, практично як накопичення статистики, інші виявляють лише окремі його ефекти тощо. Опираючись на узагальнені наукові підходи різних авторів до визначення категорії ризику, слід їх систематизувати – ймовірнісний, нерозривний, цільовий, ресурсний, ситуативний, синтезний (табл. 1.1).

Таблиця 1.1

Наукові підходи до тлумачення поняття „ризик”

Науковий підхід	Тлумачення поняття
Ймовірнісний	Потенційні можливі втрати, непевність у бажаному результаті, загроза несприятливих ефектів
Нерозривний	Постійна необхідність переборювати перешкоди задля досягнення визначеної мети
Цільовий	Можливість невизначеного відхилення від поставленої мети
Ресурсний	Загроза втрати, частини активів, недоотримання доходів, необхідність додаткових ресурсних витрат
Ситуативний	Ситуативна характеристика умов діяльності підприємства, що передбачає невизначеність генерування ефектів
Синтезний	Врахування багатьох кількісних та якісних індикаторів, для ідентифікації ризику та управління ним

Примітка: складено на основі [23].

Акцентуємо, що в сучасних економічних реаліях більш доцільним, вважаємо тлумачення ризику у контексті інтегрального підходу, що враховує багатоаспектність та змістовність цієї категорії. Тобто, ризик слід окреслювати не лише у контурі позитивних ефектів на прибутки чи фінанси підприємства, а й у зрізі ймовірнісних відхилень від запланованих бізнес-процесів та можливості примноження ціннісних показників підприємства, які у стратегічному горизонті подій визначатимуть приріст його дієвості та ефективності. Зважаючи на означене, окреслимо сутнісні характеристики „ризику” [9 с 33; 21; 167]: ризику притаманна економічна природа та невизначеність ефектів прояву; генерується постійно; коливання від бажаних мети та параметрів; можливість непередбачуваних, зумовлених обраними альтернативами результатів; не прогнозованість; незворотність прояву ефектів, результат яких не залежить від рішень менеджменту підприємства; можливість кількісного обрахування його ефектів; об’єктивність прояву; зорієнтованість на стратегічні горизонти подій; конфліктність;

суперечливість; альтернативність; динамічність; результативність; взаємозв'язок різновидів ризику. Узагальнення та систематизація зовнішніх та внутрішніх джерел виникнення ризику у діяльності підприємства наведена у таблиці 1.2.

Таблиця 1.2

Узагальнення та систематизація зовнішніх та внутрішніх джерел виникнення ризику у діяльності підприємства

<table>
<tr><th>Зовнішні джерела</th><th>Внутрішні джерела</th><th>Зовнішні джерела</th></tr>
<tr><td>Прямого впливу</td><td>Об'єктивні</td><td>Опосередкованого впливу</td></tr>
<tr><td>Природно-кліматичні та форс-мажорні кризові явища (кліматичні, воєнні, екологічні, пандемія тощо)</td><td rowspan="5">Забезпеченість підприємства ресурсами та ефективність їх використання
Розробка, впровадження нових технологій, інноваційних рішень тощо
Якість і рівень маркетингової діяльності
Рівень прибутковості підприємства
Витрати виробництва та обігу
Якість та конкурентоспроможність продукції
Продуктивність праці
Система оплати праці</td><td rowspan="2">Непередбачені зміни в міжнарод-них відносинах</td></tr>
<tr><td>Нормативно-правове поле у телекомунікаційній сфері</td></tr>
<tr><td>Нестабільність економічної (фінансової, податкової, зовнішньо-економічної тощо) політики</td><td rowspan="3">Непередбачені зміни у процесі ведення бізнесової діяльності
Недотримання положень стратегії розвитку, тактичного й оперативного планування, або їх відсутність
Недостатність бізнес-інформації на підприємстві
Географічна локація виробничих потужностей підприємства</td><td rowspan="2">Політична ситуація у країні</td></tr>
<tr><td>Науково-технічний прогрес</td></tr>
<tr><td>Непередбачені дії органів державної влади та місцевого самоврядування</td><td>ПІДПРИЄМСТВО</td></tr>
<tr><td>Зміна кон'юнктури внутрішнього і зовнішнього ринків</td><td rowspan="4">Недостатня пристосованість (маневреність) підприємства до змін конкурентного середовища
Помилки під час прийняття та реалізації управлінських та виробничих рішень
Помилки під час ідентифікації ризиків та реалізації стратегій управління ризиками
Неефективна робота управлінської та інших служб
Інтелектуальний потенціал, рівень професійного досвіду, рівень і якість знань, компетентність управлінських кадрів та інших фахівців
Система індивідуальних інтересів та мотивації у ділових ситуаціях</td><td rowspan="4">Непередбачені зміни економічної ситуації у країні, регіоні, галузі</td></tr>
<tr><td>Вплив конкурентного середовища</td></tr>
<tr><td>Зміни у відносинах з постачальниками, діловими партнерами, клієнтами</td></tr>
<tr><td></td><td>Суб'єктивні</td></tr>
<tr><td></td><td>Внутрішні чинники</td><td></td></tr>
</table>

Примітка: розроблено автором на основі [37, 157, 185].

Підтримуємо тезу, що сучасні виклики зумовлюють специфіку прояву ризику [28]:

„ризики набули тотального, загального та глобального характеру;

економічне середовище стає ризиковим (конкуренція, кон'юнктура, цінова нестабільність тощо);

дедалі більше виникає необхідність ухвалення миттєвих одноосібних рішень;

ризик стає об'єктом управління завдяки використанню: резервів, страхування, диверсифікації, лімітування, нормування й хеджування" [28].

Кожне підприємство має адаптуватись до непередбачуваних кризових, швидких, глибоких деформацій економічного простору, що притаманне для нашої країни, зберігаючи свої функції та характеристики. Виконання означених вимог можливе з використанням механізмів і технологій управління ризиком.

Узагальнене окреслення сутності категорії „управління" зводиться до наступного: управляти означає „…керувати, спрямовувати діяльність будь-кого, будь-чого" [17]; „управління – це свідомий цілеспрямований вплив з боку суб'єкта на об'єкт, що здійснюється задля спрямування їх дії у потрібне русло для отримання бажаного результату" [13]; „управління скеровує дію, результатом якої є зміна керованого процесу, предмета чи явища, їх перетворення, перехід із одного стану в інший" [83];

Сам термін „управління ризиками" розглядається в багатьох наукових вітчизняних та зарубіжних розвідках. Так, Устенко О.Л. [161], обґрунтовує „управління ризиком", „як процес впливу на суб'єкт господарювання, при якому забезпечується максимально широкий діапазон охоплення ризиків, їх обґрунтоване прийняття та зведення ступеня їх впливу до мінімальних меж, а також розробка стратегії поведінки в разі реалізації конкретних видів ризику [161]. Гранатуров В.М. [33] визначає „управління ризиком" як „сукупність методів, прийомів, заходів, що дозволяють прогнозувати настання ризикованих подій, вживати заходів щодо виключення або зниження негативних наслідків їх настання" [33]. Штефанич Д.А. [159], надає ширше формулювання „управління ризиком це сукупність дій економічного, організаційного та технічного характеру, спрямованих на визначення видів, чинників, джерел ризику, оцінку їх величини, розробку та реалізацію заходів щодо зменшення рівня та запобігання можливих втрат" [159].

Черненко Ю. О. [166], переконує, що „метою управління ризиками є забезпечення необхідного рівня стійкості та адаптивності підприємства до можливих загроз для його стабільного функціонування" [166]. Швець Ю. О. [169] окреслює „управління ризиками" через здійснення ключових функцій підприємства [169]. Підтримує такий підхід О. М. Лозовський [98]. На противагу такому функціональному підходу, Лук'янова В.В. [100] надає сутнісне тлумачення терміну „управління ризиками" за допомогою критеріїв і регламентів ухвалення управлінських рішень у цьому процесі.

Опираючись на дослідження науковців та зважаючи на мету нашого дослідження підтримаємо, що „управління ризиками будь якого підприємства,

це „цілісна система взаємопов'язаних елементів, що відображають процеси, спрямовані на діагностику, превенцію, нейтралізацію і мінімізацію ризиків та джерел їх генерування на всіх ієрархічних рівнях управлінського впливу" [40]. Таке визначення дає можливість уникнути логічних суперечностей при побудові механізму управління ризиками, формуванні відповідних методів, підходів, індикаторів діагностики тощо. Ключові принципи, якими слід керуватися при формуванні системи управління ризиками продемонстровано на рисунку 1.3.

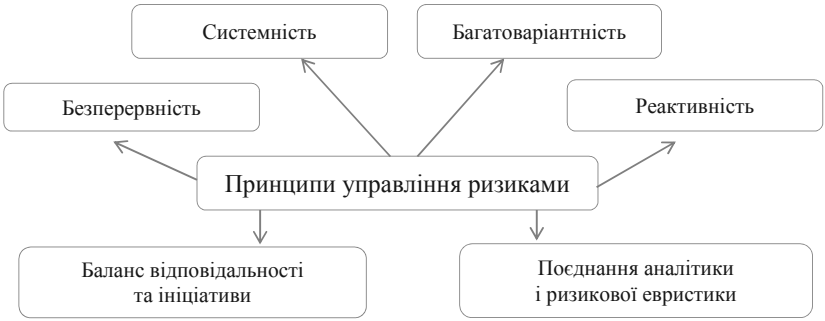


Рис. 1.3. Принципи управління ризиками підприємства
Джерело: складено за інформацією наведеною у додатках та [67].

„Ключовим завданням управління ризиками підприємства вважається встановлення оптимального рівня ризику на основі врахування чинників зовнішнього та внутрішнього середовища" [152]. Вочевидь, що результативність досягнення мети та виконання завдань управління ризиками зумовлюється адекватністю класифікації ризиків. В наукових публікаціях знаходимо багато пропозицій щодо класифікації ризиків підприємства, підгрунтям яких є різноманітні ознаки (додаток).

Узагальнена класифікація ризиків підприємства представлена на рисунку 1.4. На основі пропозицій науковців [9, 13, 23, 34, 37], сформулюємо низку узагальнень:

діапазон та асортимент ризиків підприємства залежить від складності його організаційної структури, різноманітності комунікаційних ланцюгів та стану його внутрішнього і зовнішнього середовища;

найбільш детальні класифікації ризиків, вважаємо громіздкими і незручними для практичного використання;

під ідентичною назвою різні дослідники мають на увазі різні ризики, при цьому спостерігаються значні розбіжності у визначенні їх сутності;

багато класифікаційних ознак штучно додано за рахунок суто теоретичних ознак, які неможливо використати на практиці;

не може існувати універсальної для усіх підприємств класифікації ризиків, водночас існують ознаки, що є спільними для усіх підприємств.

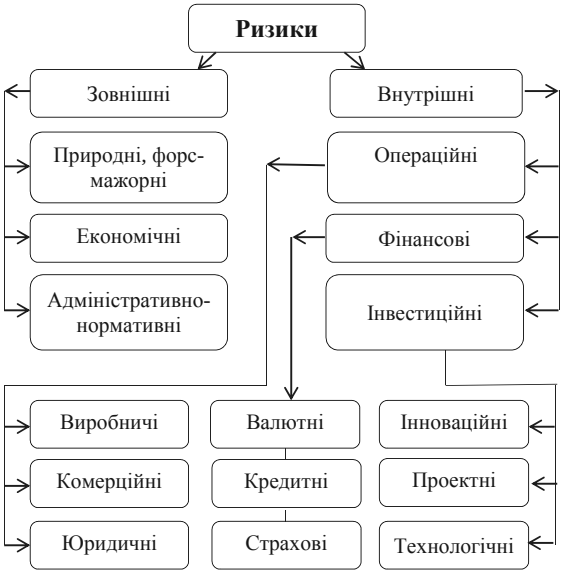


Рис. 1.4. Узагальнена класифікація ризиків підприємства
Примітка: сформовано за [34, 167].

Саме, підприємство вважається базисом будь якої національної економіки. Господарський Кодекс України визначає, що „підприємство – самостійний суб'єкт господарювання, створений компетентним органом державної влади або органом місцевого самоврядування, або іншими суб'єктами для задоволення суспільних та особистих потреб шляхом систематичного здійснення виробничої, науково-дослідної, торговельної, іншої господарської діяльності" [32]. У навчальному посібнику, більш детально будемо розглядати управління ризиками в телекомунікаційних підприємствах, тому, доцільно враховувати „особливості функціонування самого телекомунікаційного підприємства (організаційний дизайн, обсяги діяльності, форму власності, ступінь діджиталізації, вплив ризикоформуючих чинників тощо)" [184].

Специфіка ІТ-послуги й ІТ-продуктів зумовлюють і специфіку функціонування підприємств, притаманних їм ризиків та відповідно й особливостей управління ризиками (додаток). Передусім, ринок послуг на якому вони функціонують, вважається інноваційно ємким через стрімкий поступ цифрових технологій. Окрім того, високий попит через широке споживання послуг і продуктів пояснюють наявність гострої конкурентної боротьби між телекомунікаційними підприємствами, що вимагає від них розвивати сучасну технічну інфраструктуру, мати потужне цифрове обладнання й налагоджену комунікаційну мережу зі споживачами.

Водночас, оскільки, надання телекомунікаційної послуги відбувається одночасно із її споживанням, це генерує високу ресурсну залежність підприємств щодо можливості виробляти і надавати якісні телекомунікаційні послуги.

Окреслимо характерні атрибути діяльності телекомунікаційних підприємств: наявність широкого спектру та асортименту ризиків; нестача компетентного персоналу, висока плинність кадрів; якісно нові вимоги до компетенцій працівників; можливість дистанційної роботи фахівців без втрат продуктивності праці; необмежена масштабованість діяльності; низька частка у собівартості продукованих послуг та продуктів матеріальних витрат; необхідність використання сучасних технологій; необхідність своєчасної модернізації технічного та програмного забезпечення.

Врахування означених характерних атрибутів діяльності телекомунікаційних підприємств при управлінні їх ризиками забезпечить вищу ефективність управлінських процесів, сприятиме формуванню належного організаційного, інформаційного, комунікаційного забезпечення кожного етапу та генеруванню бажаних результатів.

Підтримуємо позицію тих науковців, що стверджують, що підприємства підпадають під вплив тих самих ризиків, як і інші підприємства різної галузевої належності, водночас, вони підпадають під вплив специфічних ризиків. Так, операційний ризик телекомунікаційних підприємств, може бути пов'язаний з неналежним виконанням зобов'язань щодо надання послуг, розробки програмного забезпечення через внутрішні проблеми. Тобто цей ризик, доцільно розкривати як специфічний.

Деякі вчені [29, 99] обгрунтовують наступні групи джерел ризику, що притаманні підприємствам: „технологічні, пов'язані з ІТ-інфраструктурою; втрати кадрового потенціалу; втрата або витік інформації; соціальні; проектні; юридичні; ринкові" [99]. Цікаві пропозиції щодо типології джерел ризику телекомунікаційних підприємств надають інші науковці [60].

Метою управління ризиком підприємств доцільно визначити підвищення ймовірності отримання позитивних результатів за рахунок зниження ймовірності невдач. Відповідно такого означення мети управління ризиком підприємств, дослідники переважно виокремлюють види ризиків та їх джерел (додаток). Так, дослідники [90, 99, 114] окреслюють „три групи ризиків: ризики, пов'язані з якістю розроблюваного продукту; ризики, пов'язані зі швидкістю розробки; ризики, пов'язані з бюджетом, який виділяється на розробку" [90, 99, 114]. Тобто, акцентується увага на строках, якості послуг (продукції) та бюджет. Підтримують такий підхід інші вчені [95, 163], які вважають ці ризики специфічними.

Нині, цифровізація бізнес-процесів вважається необхідною умовою, для успішного функціонування усіх підприємств та споживачів, тому вони намагаються впровадити діджиталізацію у найкоротші часові терміни, що пояснюється загостренням конкурентної боротьби та прагненням генерування додаткових конкурентних переваг. Цим пояснюється і посилення вимог до

якості ІТ- послуг та ІТ-продуктів, що впливає на можливості їх модернізації, інтеграції та розширення клієнтського кола.

До специфічних ризиків телекомунікаційних підприємств відносять [95, 163] „помилки при розрахунках, порушеннях строків надання інформації, збоїв в програмному забезпеченні, втрата бази даних, тобто технологічні ризики". Звертаємо увагу, що цими ризиками складно управляти, оскільки вони не документуються і не висвітлюються підприємствами. Вагомим ризиком підприємств є кадровий ризик, оскільки він зумовлений плинністю персоналу та необхідною високою їх кваліфікацією та рівнем їх перепідготовки.

Ринковий ризик пояснюється деформаціями економічного простору, змінами кон'юнктури. З однієї сторони телекомунікаційний ринок функціонує під дією чинників, які вважаються типовими для усіх підприємств, а з іншої – їх специфіка та темпи впливу помітно змінюють параметри функціонування. Зокрема, це зумовлено впровадженням і швидким розповсюдженням хмарних обчислень, потужного використання мобільних пристроїв та сучасних інформаційно-комунікаційних технологій, широкого використання соціальних мереж в бізнесі. Неадекватне врахування означених чинників може звузити попит на окремі ІТ-послуги та ІТ-продукти, що зумовить економічні втрати через коливання цін. Незважаючи на високі темпи розвитку телекомунікаційної сфери, нормативно-правове поле її функціонування в Україні почало формуватися та удосконалюватися лише протягом останніх років. Часті коливання нормативно-правового поля щодо функціонування підприємств, зокрема в регламентній, податковій сфері, пояснюють генерування високих юридичних ризиків.

Типові бізнес-процеси підприємств складаються з трьох основних блоків: процеси розвитку, операційні процеси та процеси підтримки (рис. 1.5). Крім фінансових, маркетингових та управлінських ризиків, вагома частка втрат підприємств визначається ризиками операційної діяльності, тобто, ризиками бізнес-процесів, безпосередньо пов'язаних із наданням ІТ - послуг чи ІТ – продуктів своїм клієнтам. Тому операційні ризики відносяться до суттєвих ризиків. До таких ризиків можна віднести:

1) *ризик основної діяльності*, спричинений технічними питаннями, що зумовлюють зростання вартості електроенергії, сировини та матеріалів, витрат на охорону навколишнього середовища;

2) *ризик недостатньої кваліфікації працівників* та низької продуктивності;

3) *техніко-технологічний ризик*, який включає недосконаліть бізнес-процесів, помилки тарифікації, не оптимальність маршрутизації трафіку, збої технологічного обладнання, шахрайство, дії конкурентів, розвиток мереж, впровадження нових послуг.

Так, зокрема, за оцінками експертів, „у результаті реалізації ризикових подій операційної діяльності компанія-оператор зв'язку може втратити близько 15% своїх доходів, що негативно вплине на інвестиційну привабливість компанії" [150 с.170].

Рис. 1.5. Специфічні ризики підприємств у зрізі бізнес-процесів.
Примітка: сформовано за [99, 114, 150].

Крім операційних ризиків для підприємств особливо характерні інвестиційні ризики, оскільки особливі умови конкуренції ринку послуг змушують вкладати кошти в інноваційні проекти, створені задля розвитку нових технологій. До таких новаторських технологій та послуг, що надаються на їх основі, можна віднести: широкосмуговий доступ до Інтернету, послуги інтелектуальної мережі зв'язку, цифрове телебачення, організація відео конференцій, пропуск трафіку за допомогою віртуальних приватних мереж та інші. Головним заходом подолання наслідків та ризиків кризи стало скорочення інвестиційних програм. Систематизація ризиків підприємств наведена у додатку. Між виокремленими блоками специфічних ризиків (додаток) проявляється взаємозалежність. Представлений систематизований опис специфічних ризиків для функціонування підприємств надасть можливість сформувати індикатори цих ризиків для проведення діагностики та виявити результативність управління ризиками підприємств.

1.2. Управління ризиками в проектах цифровізації підприємств

Будь-який бізнесовий проект цифровізації підприємств, тісно переплітається з невизначеністю і ризиками.

Невизначеність в проекті цифровізації – це недолік або відсутність інформації, знань або розуміння можливих наслідків дій, що робляться, рішень або подій. Результатом присутності невизначеності є ризики. Один з процесів в управлінні проектом цифровізації – управління ризиками. Як і інші процеси, він є „наскрізним" для проекту і присутній на всіх стадіях його життєвого циклу.

Відповідно до визначення американського стандарту в галузі управління проектами PMBOK, ризик проекту – це невизначена подія або умова, яка в разі виникнення має позитивний або негативний вплив, щонайменше, на одне з обмежень проекту, наприклад, терміни, вартість, обсяги або якість. Підкреслюється значимість того, що ризик у проекті може мати не тільки негативний, але і позитивний вплив на проект, тобто приводити до поліпшення якісних і кількісних характеристик кінцевих цілей проекту. Відповідно, можна виділити негативні ризики, позитивні ризики і непередбачені обставини:

1. Негативні ризики – загрози, іншими словами, події, що ведуть до погіршення якості виконання проекту, що вимагають залучення додаткових витрат ресурсів і часу або, ймовірно, що знижують якісні характеристики кінцевого результату.

2. Позитивні ризики – можливості, або події, що надають шанс поліпшити якість реалізації проекту і досягти цілей, можливо, з меншими витратами ресурсів і часу або більш високою якістю.

3. Непередбачувані обставини – ті, що неможливо було або не змогли передбачити на стадії ідентифікації ризиків.

Ризик може бути викликаний однією або декількома причинами і в разі виникнення будь-якої з цих точно не відомих заздалегідь подій може вплинути на вартість проекту цифровізації, його розклад або виконання. Ризики

визначаються як зовнішніми по відношенню до проекту цифровізації або підприємства – умовами середовища, – так і внутрішніми – умовами реалізації проекту цифровізації.

Для підвищення якості виконання проекту цифровізації і досягнення кінцевих цілей менеджер проекту реалізує процес управління ризиками.

Управління ризиками – це систематичний процес зниження невизначеності та управління ймовірністю подій в проекті. Мета управління ризиками проекту цифровізації – підвищення ймовірності виникнення і впливу сприятливих подій і зниження ймовірності виникнення і впливу несприятливих для проекту подій.

Весь процес управління ризиками проекту цифровізації поділяється на окремі підпроцеси, які виникають як мінімум один раз в кожному проекті, а деякі реалізуються на декількох стадіях проекту, носячи ітеративний характер:

1. Планування управління ризиками – інтегруючий процес вибору підходу, планування і виконання операцій з управління ризиками проекту. Реалізується на стадії планування проекту цифровізації.

2. Ідентифікація ризиків – визначення того, які ризики можуть вплинути на проект, і документальне оформлення їх характеристик. Виникає на стадії планування проекту цифровізації, але носить повторюваний характер, виникаючи періодично для поповнення реєстру ризиків проекту в міру його реалізації.

3. Якісний аналіз ризиків – розташування ризиків за ступенем їх пріоритету для подальшого аналізу або обробки шляхом оцінки і підсумовування ймовірності їх виникнення та впливу на проект цифровізації.

4. Кількісний аналіз ризиків – кількісний аналіз потенційного впливу ідентифікованих ризиків на загальні цілі проекту цифровізації.

5. Планування реагування на ризики – розробка можливих варіантів і дій, що сприяють підвищенню сприятливих можливостей і зниження загроз для досягнення цілей проекту цифровізації.

6. Моніторинг та управління ризиками – відстеження ідентифікованих ризиків, моніторинг залишкових ризиків, ідентифікація нових ризиків (і пов'язаний процес якісного і кількісного аналізу, а також вироблення планів реагування), виконання планів реагування на ризики і оцінка їх ефективності на протязі життєвого циклу проекту цифровізації.

Всі проекти цифровізації різняться, і кращий метод виявлення потенційних ризиків всередині складного проекту – звернутися до досвіду минулих проектів в тій же сфері. Навіть в різних галузях виробництва існує багато однакових або схожих потенційних ризиків.

Перший підхід – повністю проаналізувати різні сегменти проекту цифровізації: масштаб, устаткування, технологія, існуючі дані, люди, терміни, бюджет.

Потім розбити кожен розділ проекту на більш дрібні фрагменти. Груповий пошук ідей з невеликою групою членів команди, що представляють різні відділи і групи, може принести користь. Він не повинен займати багато часу, але вкрай важливий для успішного управління проектом цифровізації.

Масштаб. Суть масштабу – визначення того, що входить або не входить в документ бізнес-вимог. Тому сегменти, які можуть генерувати проблеми, поставлять питання, пов'язані з тим, що написано або не написано в цьому документі. З цієї причини першими виявленими ризиками можуть бути „недолуго визначені бізнес-вимоги", „відсутність досвідченого персоналу, що визначає вимоги" або „бізнес-вимоги, не затверджені підприємством".

Устаткування. Цей сегмент аналізу повинен стосуватися обладнання, необхідного для виконання проекту цифровізації, а не того, що надається або є кінцевим результатом проекту. Воно може включати в себе комп'ютерну техніку або устаткування для виготовлення кінцевого продукту або шерег інших варіантів, в залежності від конкретного проекту. При виявленні ризиків в даному розділі потрібно розглянути такі ризики, як: „яка надійність обладнання", „наскільки легко замінюється обладнання в разі його пошкодження чи поломки", „яка вартість заміни несправного обладнання".

Технологія. У проектах цифровізації, направлених на розробку програмного забезпечення, даний розділ охоплює всі пов'язані з комп'ютерами сфери, крім фізичної апаратури. Потрібно перевірити залежності пакетів програм (внутрішні та зовнішні) і системи управління базами даних. Для довгострокових проектів оновлення до різних версій програмного забезпечення може вплинути на терміни або викликати непередбачені витрати, якщо воно вимагає додаткового персоналу або перенавчання наявного персоналу.

Існуючі дані. Чи потребують існуючі дані переходу на нову систему – якщо так, то чи працюватиме використаний раніше відпрацьований метод, або потрібно принципово нове рішення? Все, що не робилося раніше, ймовірно, несе високий ризик; особливо якщо існуючі дані є пропрієтарними, тому немає досвіду і знань з попередніх проектів всередині або поза організацією, до яких можна звернутися.

Люди. Наскільки важливий існуючий персонал для успіху проекту цифровізації? Чи мають вони спеціальні знання, які було б важко або дорого знайти де-небудь ще? Чи висока нинішня плинність кадрів, або ж існуючі групи міцні, добре мотивовані і ймовірно залишаться протягом усього проекту? Керівник великого глобального проекту цифровізації може навіть не знати проектні групи в різних місцях, а лише підтримувати контакт з локальними керівниками проектів. Проте для невеликого проекту знання складу проектної групи дуже важливе в оцінці потенційних ризиків.

Строки. Наскільки точні оцінки для цілого проекту цифровізації і для кожної окремої задачі? Чи відрізняється проект від усього, що робилося раніше, і тому є всі оцінки приблизними, або, що ще гірше, чистими здогадками? Чи продиктовані строки комерційною необхідністю, як у випадках, коли випуск продукту на ринок раніше конкурентів є вагомим чинником? Чи було дозволено групам, які мають знання для надання точних оцінок, зробити їх? Зазначені чинники впливають на тип і ймовірність виникнення ризиків у контурах термінів.

Бюджет. Чи був бюджет визначений більше комерційною необхідністю, ніж реальною вартістю, необхідною для виконання проекту цифровізації? Обмежений бюджет не обов'язково зводить на нівець успіх проекту. Досвідчений керівник проекту має навички, необхідні для отримання максимальної користі з обмеженого бюджету і для мінімізації ризиків всередині такого проекту.

Багато чинників, які недосвідчені керівники проектів цифровізації вважають такими, що створюють більш ризикований проект, насправді легко управляються, оскільки вони виникають досить часто, наприклад, обмежені ресурси часу або бюджету. Ризиком швидше є те, що виникає рідко, або революційні нові цифрові технології або продукти, що збивають проект з вірного шляху.

Виявлення ризиків в проекті цифровізації має вирішальне значення для успішного управління ними, і описані вище сфери є найважливішими для аналізу при виявленні ризиків.

Кожен керівник проекту і бізнес-лідер хоче бути обізнаному практиці і принципах ефективного управління ризиками. Якщо керівництво програми або проекту знає, як визначати ризики і як з ними поводитися, то, таким чином, можна запобігти зайвим складнощам у майбутньому і підготуватися до них.

Можна виділити декілька принципів, які винайдені не для того, щоб давати інструкції, а для того, щоб забезпечити підтримку керівнику, яка надає можливість підприємствам розвивати свій власний курс, процес, стратегію і план.

1) Організаційне середовище. Усі підприємства відрізняються одне від одного. Це є основним принципом всіх загальних методів управління, включаючи підхід PRINCE2 і метод управління успішними програмами проектів, так само як управління ризиками. Керівникам проектів цифровізації, керівникам програм і менеджерам за ризиками необхідно розглянути специфічне середовище підприємства для того, щоб гарантувати повну ідентифікацію ризиків і відповідні процедури роботи з ними. Термін „організаційне середовище" містить в собі політичний, економічний, соціальний, технологічний, правовий аспекти і відноситься до зовнішнього середовища підприємства.

2) Залучення учасників. Керівній команді легко засвоїти і також легко забути, що зацікавлені особи є ключовими учасниками в щоденних процедурах бізнесу, а короткострокові і великі ділові проекти цифровізації змінюють програму. Розуміння ролі окремих учасників і їх залучення є ключовим моментом для досягнення успіху. Учасники повинні бути інформовані про ризики проекту настільки, наскільки це можливо. Усередині організаційного середовища залучення учасників має на увазі особу учасника і його роль, ступінь впливу на підприємство і за його межами, рівень інвестицій, тип, можливості і потенційний вплив ризику.

3). Організаційні цілі. Ризик є в діях і цілях підприємства. Приміром, дощ є негативним ризиком для пікніка, позитивним – для посушливого ділянки і не є ризиком для екіпажу субмарини. Персональна відповідальність

за управління ризиками лежить на лідері, керівника проекту, і стосується цілей підприємства, для гарантування ретельного підходу.

4). Підхід до управління ризиками. Процес, політика, стратегія і план в межах структури управління ризиками забезпечують загальні принципи і шаблони всередині окремого підприємства. Ці принципи ґрунтуються на досвіді управління і на знаннях і дослідженнях професійних менеджерів за ризиком широкого шерегу підприємств. Дотримання кращої практики гарантує, що окремі особи, залучені до управління ризиками та в організаційну діяльність, здатні вчитися на своїх помилках, експериментах і на уроках інших.

5). Звіт. Точне і чітке надання даних і їх передача відповідним співробітникам, керівникам і зацікавленим особам є ключовим чинником успішного управління ризиками. Методологія управління ризиками забезпечує стандартний зразок і перевірену структуру управління учасниками, а також частотою і змістом області ризику.

6). Ролі та відповідальності. Для кращої практики управління ризиками істотним чинником є чітке визначення ролі управління і відповідальності. Індивідуальні функції і відповідальність повинні бути очевидними всередині підприємства та за його межами. Це важливо для термінів організаційного управління та для гарантії того, що вся необхідна відповідальність покладена на відповідну особу.

7). Структура підтримки. Структура підтримки – це забезпечення всередині підприємства стандартних принципів, інформації, навчання та фінансування індивідуального управління ризиками, які можуть виникнути в будь-який специфічній галузі або в будь-якому проекті цифровізації. Ця структура може включати централізовану команду управління ризиками, стандартний підхід і кращі практичні принципи звіту і перегляду організаційних ризиків.

8). Цикл перегляду. Цикл перегляду пов’язаний з необхідністю отримання показників попереднього сповіщення про настання ризикової події. Він забезпечує постійний перегляд встановлених ризиків і гарантує, що менеджери залишаться відкритими для виявлення нових ризиків.

9). Подолання бар’єрів на шляху управління ризиками. Будь-яка успішна стратегія вимагає ретельного розгляду можливих перешкод для здійснення проекту цифровізації. Загальні питання включають в себе:

встановлення ролей, відповідальностей, підзвітності та власності;

відповідний бюджет для впровадження підходу і виконання діяльності;

відповідне і доступне навчання, інструменти і методи;

орієнтування на управління ризиками, ознайомлення та навчальні процеси.

Регулярне оцінювання підходу управління ризиками, включаючи всі перераховані вище питання.

10). Підтримуюча культура. Управління ризиками має на увазі багато різних сфер і аспектів організаційної діяльності. Підтримуюча культура дуже важлива для того, щоб всі відповідальні особи відчували впевненість,

обговорюючи і керуючи ризиками. Підтримуюча культура управління ризиками буде також включати в себе оцінку та винагороду компетентності відповідних осіб.

11). Постійне поліпшення. Підприємство, яке прагне успіху не стоїть на місці, а постійно розвивається.

Ефективна політика управління ризиками включає здатність до переоцінки і удосконалення. На практичному рівні потрібно призначення окремої особи або групи осіб відповідальними за гарантію того, що політика управління ризиками і методика відповідає сучасним вимогам цифровізації.

Ризики управління проектом цифровізації складаються з операційних, фінансових та інвестиційних.

Основними джерелами операційного ризику є виробничий брак, погані умови на будівельних майданчиках, виплата підвищених податків, відрахувань і штрафів, помилки планування, брак координації робіт, зміни в персональному складі керівництва проектом, інциденти, нещасні випадки, дефіцит і відсутність персоналу необхідної кваліфікації для виконання робіт проекту цифровізації. У вітчизняних умовах до цих чинників додається низька дисципліна поставок, перебої з паливом і електроенергією, фізичний і моральний знос устаткування.

Фінансовий ризик враховує грошові витрати, збитки і втрати. Особливістю фінансового ризику є ймовірність настання збитку в результаті проведення яких-небудь операцій у фінансово-кредитній і біржовій сферах, здійснення операцій з фондовими цінними паперами, тобто ризику, що випливає з природи цих операцій. До фінансових ризиків відносяться наступні:

кредитний ризик – небезпека несплати позичальником основного боргу і відсотків, належних кредитору;

процентний ризик – небезпека фінансових втрат комерційними банками, кредитними установами, інвестиційними фондами в результаті перевищення процентних ставок, виплачуваних ними по залучених засобах, над ставками за наданими кредитами;

валютний ризик – небезпека валютних втрат, пов’язаних зі зміною курсу однієї іноземної валюти по відношенню до іншої, у тому числі національній валюті при проведенні зовнішньо-економічних, кредитних та інших валютних операцій.

Фінансовий ризик, як і будь-який ризик, має математично виражену ймовірність настання втрат, яка спирається на статистичні дані і може бути розрахована з досить високою точністю. Щоб кількісно визначити величину фінансового ризику, необхідно знати всі можливі наслідки якої-небудь окремої дії і ймовірність самих наслідків. Імовірність означає можливість отримання певного результату. Стосовно до економічних задач методи теорії ймовірності зводяться до визначення значень імовірності настання подій і до вибору з можливих подій самого кращого виходячи з найбільшої величини математичного очікування. Інакше кажучи, математичне очікування якої-

небудь події дорівнює абсолютній величині цієї події, помноженої на ймовірність його настання.

У будь-якій цифровізації підприємств завжди існує небезпека втрат, яка випливає із специфіки тих чи інших технологічних операцій. Небезпека таких втрат являє собою комерційні (підприємницькі) ризики. Комерційний ризик означає невпевненість у можливому результаті, невизначеність цього результату діяльності. Комерційні ризики пов'язані, зокрема, з непередбачуваністю зміни закупівельної ціни товарів, зростанням витрат обігу, втратами і псуванням сировини, матеріалів і устаткування при зберіганні і транспортуванні.

Залежно від галузі розрізняють чисті, (прості) і спекулятивні комерційні ризики. Наявність чистих ризиків означає можливість збитку або „нульового" результату: цей ризик розрахований тільки на програш. Спекулятивні ризики виражають можливості одержання як позитивного, так і негативного результату.

Інвестиційний ризик можна визначити як відхилення фактичного доходу від очікуваного доходу. Інвестиція вважається не ризикованою, якщо дохід по ній гарантований. Одним з прикладів не ризикованою інвестиції є цінні папери казначейства, оскільки шанс того, що уряд не зможе викупити свої цінні папери, практично дорівнює нулю. Навпаки, при вкладенні коштів у проект, пов'язаний, наприклад, з виробництвом принципово нового цифрового продукту, або виходом на новий ринок, або придбанням цінних паперів якого-небудь підприємства, завжди існує певна ймовірність того, що в результаті непередбачених обставин виплата доходів за ним не буде проведена або проведена не в повному обсязі.

Загальний або сукупний ризик являє собою суму всіх ризиків, пов'язаних із здійсненням будь-якого проекту цифровізації і класифікується за різними ознаками. За тимчасового ознакою виділяються наступні види загального ризику:

короткострокові – пов'язані з окремими фазами життєвого циклу проекту і припиняються разом із завершенням фази;

довгострокові – пов'язані з декількома або всіма фазами проекту.

За масштабом і ймовірності втрат розрізняють ризики:

високі – висока ймовірність настання ризикових подій і великі масштаби втрат і витрат на подолання наслідків ризикової події;

слабкі – низький рівень втрат.

Залежно від ступеня впливу на фінансове становище проекту виділяються:

допустимий ризик – загроза уповільнення виконання проекту або збільшення його вартості в допустимих межах;

критичний ризик – ризик, пов'язаний із загрозою істотного відхилення проекту по термінах і вартості;

катастрофічний ризик – найнебезпечніший ризик, що приводить до високої ймовірності дострокового припинення проекту або нанесення непоправної шкоди соціально-природним системам.

За сферами прояву виділяють такі ризики:

економічні – пов'язані зі зміною економічних чинників здійснення проекту;

політичні – пов'язані зі зміною політичного курсу країни, регіону;

соціальні – пов'язані з соціальними проблемами (наприклад, ризик страйків);

екологічні – пов'язані із загрозою екологічних катастроф і лих;

нормативно-законодавчі – пов'язані зі змінами законодавства та нормативної бази.

Залежно від джерел виникнення та можливості усунення проектні ризики бувають:

несистемні (специфічні) ризики – ризики, викликані такими особливими для проекту подіями, як дефіцит сировини, матеріалів, робочої сили, успішні або невдалі програми взаємодії зі стейкхолдерами проекту, невиконання договорів субпідрядниками, неефективні аутсорсингові заходи, помилки у прийнятті управлінських рішень, аварії, викликані порушенням норм, правил, технологій та багато іншого. Такі ризики носять індивідуальний, специфічний для кожного проекту цифровізації характер, і управління ними в чому залежить від досвіду, знань і навичок менеджера проекту;

системні ризики виникають із зовнішніх подій, що впливають на ринок в цілому: це війна, інфляція, економічний спав, висока ставка відсотка тощо. На систематичний ризик припадає до 50% загального ризику проекту. Системні ризики, що мають спільні корені, але різні прояви у різних проектах, легше прогнозуються і для них легше скласти загальні правила і рекомендації, які мінімізують їх негативний вплив на проект.

Ризики виникають тоді, коли діють чинники ризику – виникають ситуації, що породжують ризики. Сам по собі чинник ризику не веде до зриву робіт за проектом або їх подорожчання, він тільки підвищує ймовірність настання несприятливої події, яка, в принципі, може і не виникнути. Чинником ризику може бути сам проект цифровізації, якщо подібні проекти підприємством не робилися. Знизити тиск цього чинника може, наприклад, запрошення досвідченого менеджера проекту.

Успіх проекту залежить від того, яку стратегію або стратегії реагування на ризики запланує і реалізує команда управління проектом цифровізації. Заплановані операції з реагування на ризики повинні:

відповідати серйозності ризику;

бути економічно ефективними в рішенні проблеми;

бути своєчасними;

бути реалістичними в контексті проекту;

бути узгодженими з усіма учасниками.

Виконання заходів з управління ризиком має бути покладено на відповідальну особу, іншими словами, конкретним ризиком управляє конкретний учасник проекту.

У стандартах управління проектами виділяються:

1. Стратегії реагування на негативні ризики (загрози);

2. Стратегії реагування на позитивні ризики (сприятливі можливості);

3. Загальні стратегії реагування на ризики;

4. Стратегії реагування на непередбачені обставини.

Будь-яка стратегія роботи з ризиком спрямована на управління або ймовірністю ризику, або наслідками ризику, або одночасно двома даними параметрами.

Стратегії реагування на негативні ризики:

Ухилення. Ухилення від ризику передбачає зміну плану управління проектом таким чином, щоб виключити загрозу, викликану негативним ризиком, захистити мету проекту від наслідків ризику або послабити обмеження, що знаходяться під загрозою (наприклад, розширити контури розкладу або зменшити зміст проекту). Деяких ризиків, що виникають на ранніх стадіях проекту, можна уникнути за допомогою уточнення вимог, отримання інформації, поліпшення комунікації або проведення експертизи. Ризики уникаються шляхом простого невиконання частини проекту. Прикладом стратегії ухилення є використання перевіреної технології замість недавно розробленої, ще не відпрацьованої технології, що, ймовірно, допоможе уникнути технічного ризику. Вибір постачальника з політично більш стабільного регіону знизить ймовірність того, що політичні ризики постачальника вплинуть на поставки для даного проекту. Опрацювання кількох альтернативних напрямків створення продукту на ранніх стадіях технологічних проектів, які згодом визначать ключовий напрямок, дозволить уникнути отримання продукту, який не буде відповідати цілям проекту. Наприклад, на ранніх стадіях концептуального визначення технології опрацьовується кілька варіантів реалізації і згодом вибирається один - оптимальний, з точки зору команди управління проектом. Цьому варіанту дається «зелене світло», і проводиться детальне опрацювання. Звичайно, це не знімає повністю ймовірність того, що обраний варіант повністю забезпечить поставлені цілі проекту, проте це виключає з подальшого опрацювання свідомо неробочі варіанти. На приклад, у разі можливого значного зсуву термінів проекту через ймовірний зрив поставок обладнання постачальником, команда проекту виключає даного постачальника з тендерного списку. Ризикова подія виключається з плану проекту, команда ухиляється від ризику.

Передача і розподіл. Передача і розподіл ризику має на увазі перекладення негативних наслідків загрози з відповідальністю за реагування на ризик на третю сторону, частково або повністю. Передача ризику просто переносить відповідальність за його управління іншій стороні, ризик при цьому не усувається. Передача відповідальності за ризик найбільш ефективна щодо фінансових ризиків. Передача ризику практично завжди передбачає виплату премії за ризик стороні, що приймає на себе ризик.

Інструменти передачі ризиків включають в себе, зокрема:

страхування;

гарантії виконання контракту;

поручительства і гарантійні зобов’язання;

прописування умов в контракті;

інше.

Умови передачі відповідальності за певні ризики третій стороні можуть визначатися в контракті. На приклад, на стадії укладення контракту на будівництво певної дослідної ділянки Замовник і Виконавець обумовлюють фіксовану вартість контракту на проведення робіт. Надалі в разі підвищення вартості будівельних матеріалів і комплектуючих Виконавець покриває дані зміни з власного прибутку. Замовник же знімає з себе цей ризик.

Більш м'яким варіантом передачі є розподіл ризиків, якому приділяється все більше уваги в останні роки. За такої стратегії відповідальність за ризик несуть обидві сторони договору при реалізації проекту. Поділ ризиків між постачальником і командою проекту ініціює взаємовигідний процес удосконалення, спонукаючи постачальників до інновацій.

Послаблення. Стратегія послаблення (пом'якшення) ризиків передбачає:

зниження ймовірності реалізації ризику;

зниження наслідків негативного впливу ризикової події до прийнятних меж – ризик або не збудеться, або збудеться, але з меншими наслідками.

Вжиття запобіжних заходів щодо зниження ймовірності настання ризику або його наслідків часто виявляється більш ефективним, ніж зусилля щодо усунення негативних наслідків, що вживаються після настання події ризику. Як приклади заходів щодо зниження ризиків можна привести:

1. Впровадження менш складних процесів, структурне спрощення, деталізацію процесів до такого рівня, який дозволить досить знизити ймовірність реалізації ризику. Крім спрощення процесів, ймовірність ризиків може знизити більш детальний опис процесів або застосування додаткових програм навчання персоналу проектів.

2. Проведення більшої кількості випробувань або реалізацію прототипів, на яких виробляється відпрацювання основних рішень проекту. Наприклад, при реалізації проектів цифровізації можливе виділення дослідної групи або ділянки, на якому проводиться перевірка розроблених технічних рішень.

3. Вибір постачальника, поставки якого носять більш стабільний характер. Вибір може здійснюватися на підставі даних архівів минулих проектів.

Стратегії реагування на позитивні ризики:

Використання. Ця стратегія може бути обрана для реагування на ризики з позитивним впливом, якщо необхідно, щоб дана сприятлива можливість гарантовано була реалізована. Дана стратегія призначена для усунення всіх невизначеностей, пов'язаних з ризиком верхнього рівня, за допомогою заходів, що забезпечують появу даної слушної нагоди в різних формах. До числа заходів прямого реагування на дану можливість належать залучення до участі в проекті більш талановитого персоналу, з тим щоб скоротити час, необхідний для його завершення, або забезпечення більш високої якості, ніж було передбачено початковим планом. На приклад, керівник проекту знає, що застосування більш якісних і сучасних вогнетривких матеріалів підвищить термін служби обладнання. Якщо у команди проекту з'явиться можливість і /

або ресурс на використання таких матеріалів, то вони вдадуться до них, і в результаті якісні характеристики даного проекту підвищаться.

Спільне використання. Спільне використання позитивних ризиків передбачає передачу відповідальності третій стороні, здатній щонайкраще скористатися можливістю, що виникла, в інтересах проекту. До числа заходів зі спільним використанням сприятливих можливостей відноситься створення партнерств зі спільною відповідальністю за ризики, команд, спеціалізованих компаній або спільних підприємств, створених спеціально для управління сприятливими можливостями.

Посилення. При застосуванні цієї стратегії змінюється «розмір» слушної нагоди шляхом підвищення ймовірності виникнення та / або позитивного впливу, а також шляхом виявлення і максимізації основних джерел цих позитивних ризиків. Для підвищення цієї ймовірності можна спробувати полегшити або зміцнити причину, яка викликає сприятливу можливість, і цілеспрямовано підсилити умови її появи. Можна також вплинути на джерела впливу, намагаючись підвищити чутливість проекту до цієї слушної нагоди.

Загальні стратегії реагування на ризики:

Прийняття. Ця стратегія означає, що команда проекту прийняла рішення не змінювати план проекту у зв'язку з ризиком або не знайшла іншої підходящої стратегії реагування на ризики, оскільки або ймовірність ризику занадто мала, або ефект від ризику надто великий і його вплив на цілі проекту в разі реалізації ставить під сумнів ключові цілі проекту. Ця стратегія може бути застосована або до загроз, або до сприятливих можливостей. Вона може бути або активною, або пасивною.

Ця стратегія використовується у випадках, коли:

виключити всі ризики з проекту малоймовірно;

наслідки ризику настільки великі, що недоцільно розробляти варіанти його передачі з метою зменшення впливу на проект;

ймовірність ризику і його наслідки малі, його можна прийняти, оскільки вартість розробки заходів з управління ризиком перевершує вартість наслідків.

Пасивне прийняття даної стратегії не передбачає проведення будь-яких запобіжних заходів, залишаючи команді проекту право діяти на власний розсуд в разі настання події ризику. Деякі способи реагування призначені для використання тільки в разі виникнення певних подій, тобто реалізації ризиків. Стосовно до деяких ризиків команда проекту може задіяти план реагування на ризики, який може бути введений в дію тільки при заздалегідь визначених умовах – якщо є впевненість і достатня кількість ознак того, що даний план буде успішно виконаний. Необхідно визначити і відстежувати події, які приводять в дію механізм реагування на непередбачені обставини, наприклад, відсутність проміжних контрольних подій або привласнення певному постачальнику високого рівня пріоритетності. Моніторинг ризиків і реалізація планів дій, в разі їх реалізації, вимагає закладання в бюджет і плани проекту резервів на ризики – резервів на відоме невідоме. Однак в будь-якому проекті цифровізації є те, що ми не могли передбачити і передбачити, – „невідоме

невідоме". Для впливу на подібні події в проекті створюється управлінський резерв (бюджетний фонд), який використовується командою управління проектом у разі виникнення подібних обставин. Яку б стратегію реагування на ризик не вибрав менеджер проекту, план реагування на ризик і формування резервів на його забезпечення проводиться до можливої реалізації ризику.

1.3. Механізм управління ризиками в підприємствах

Характерною рисою сучасного етапу поступу економіки є глибокі зміни, які проходять в усіх її сферах під впливом цифровізації, трансформаційних зрушень та глобальних перетворень. Посилення процесів нестабільності впливає на систему управління ризиками підприємств та її подальший розвиток. Враховуючи ці особливості на фоні турбулентності ринкового середовища, доцільна побудова механізму управління ризиками в підприємствах, який у процесі реалізації здатен забезпечити збалансованість бізнес-процесів й ефективне їх функціонування, що допоможе менеджменту підтримувати стійкість конкурентних позицій та ефективність функціонування підприємства через певний набір методів, інструментів, важелів, функцій та принципів.

Сама категорія „механізм" запозичена з технічної термінології та давно широко використовується в різних науках та практиках.

Так в економічній літературі вчені по різному трактують поняття „механізм", зокрема:

сукупність (або систему) формальних і неформальних правил, процедур, методів, способів, форм, важелів, функцій управління економічними відносинами різного рівня [162 с. 130];

комплексна система інструментів (правових, економічних, адміністративних, організаційних, освітніх, пропагандистських тощо), пов'язаних єдиними цілями, принципами та забезпечених відповідними ресурсами [24 с. 123];

механізм, що забезпечує взаємодію підсистеми, яка управляє, та підсистеми, якою управляють. Він складається із сукупності конкретних форм і методів свідомого впливу на економіку [35 с. 25].

Подальші дослідження механізму у контексті управління розглядаються як „механізм управління".

Так група вчених [6] трактує механізм розвитку як спеціалізований вузол механізму управління, що забезпечує динамічну зміну конфігурацій, що склалися, та набори елементів у блоках господарського механізму.

У класичному розумінні механізм, що забезпечує процеси управління ризиками, визначається найчастіше як складова механізму управління, яка, відповідно до теорії управління, повинна об'єднувати цілі управління, критерії управління, чинники управління, методи управління [171 с. 208].

Механізм управління, за ствердженням О. В. Раєвнєвої [138, с. 226], розуміється як „сукупність: засобів управління, які включають інструменти та важелі, що відповідають орієнтирам, передбачуваним наслідкам, критеріям

відбору й оцінки, обмеженням і вимогам процесу розвитку підприємства з урахуванням певної стадії циклу його розвитку; організаційних і економічних методів управління, що представляють собою способи, прийоми та технології приведення в дію та використання засобів управління" [138 с. 226].

Інший погляд на механізм управління підприємства надає О.Ю. Гаркуша [25], та характеризує його як „комплекс дій і технік організаційно-економічного характеру, спрямованих на забезпечення стійкого економічного зростання при збалансованості бізнес-процесів на основі використання певних способів, методів та інструментів управління розвитком підприємств, що відповідають специфіці їх діяльності та галузевим особливостям функціонування" [25].

Цікавий погляд на зміст механізму управління надає О.Є. Гудзь, яка розглядає його з позицій гармонізації та інноваційного розвитку у стратегічній перспективі. На думку О.Є. Гудзь, основною вимогою до формування та гармонізації механізму управління підприємства з боку системного підходу є „визначення кожного елемента системи у його зв'язку і взаємодії з іншими, виявлення впливу й властивостей її складових, визначення оптимального режиму функціонування" [38 с. 276].

Таке розуміння змісту механізму управління підсилює можливості підприємств виживати у нестабільному ринковому середовищу відповідно до цілей підприємств.

Підтримуємо підходи вчених щодо розгляду механізму управління підприємства – як сукупності дій та технік організаційно-економічного характеру, які надають можливість проектувати новий механізм функціонування із заданими властивостями під впливом різноманітних чинників, що допоможе підприємству перейти з одного стану до іншого, більш досконалого.

Зазначимо, що ефективність механізму управління підприємства, залежить від різноманітних чинників, зокрема, ступеня розвитку виробництва та раціонального споживання матеріальних ресурсів, поділу і кооперації праці, використання результатів науково-технічного прогресу, застосування інтелектуальних ресурсів, форм стимулювання та мотивації праці менеджерів та працівників підприємства тощо. Кожний зазначений чинник не створює окремого впливу на діяльність підприємства, а тільки у взаємодії з іншими, та за умов взаємного інтегрування. Застосування того чи іншого чинника без зв'язку з іншими не є доцільним. Для забезпечення стабільного економічного поступу підприємств у період несприятливих подій, необхідною складовою механізму управління вважається механізм управління ризиками.

На рисунку 1.6 наведено схему розв'язання комплексу завдань механізму управління ризиком.

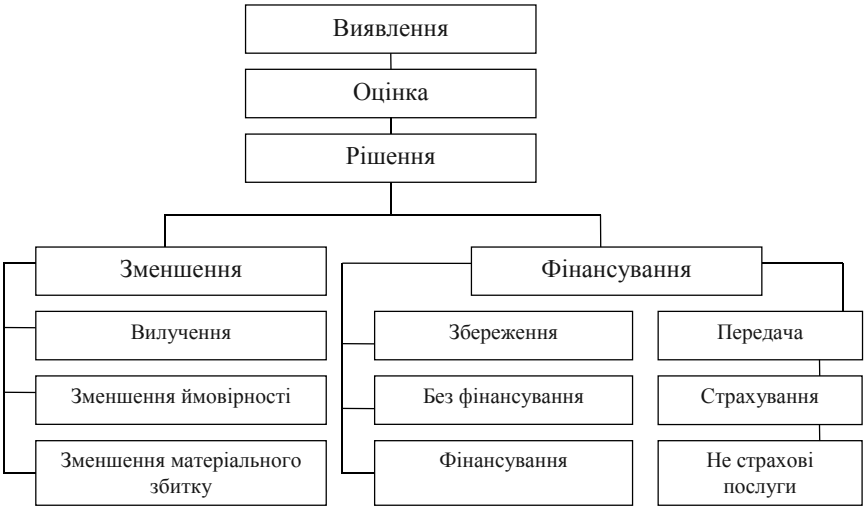


Рис.1.6. Схема розв'язання комплексу завдань механізму управління ризиком
Примітка: сформовано на основі [111 с.66-67]

Методи фінансування ризику спрямовані на компенсацію втрат і збитків, які трапляються навіть за ефективного управління ризиком, але, звичайно, такі витрати будуть меншими, ніж коли управління ризиком взагалі немає або воно неефективне [91; 111 с.66-67].

На думку Л. І. Донець механізм управління ризиком, або ризик-менеджмент (management by the risk), є специфічним видом управлінської діяльності (галуззю менеджменту), спрямованим на ефективний захист підприємства від небажаних закономірних чи випадкових обставин (подій), які у підсумку можуть негативно впливати на роботу підприємства [51].

З точки зору О. Л. Устенко механізм управління ризиком − це процес впливу на суб'єкт господарювання, при якому забезпечується максимально широкий діапазон охоплення можливих ризиків, їх обгрунтоване прийняття та зведення ступеня їх впливу до мінімальних меж, а також розробка стратегії поведінки даного суб'єкта у разі реалізації конкретних видів ризику [160].Обгрунтовуючи зміст процесу управління ризиками М. Гранатуров [33 с. 7], ототожнює його із певним механізмом та характеризує механізм управління ризиком як сукупність методів, прийомів, заходів, що дозволяють певною мірою прогнозувати настання ризикованих подій і вживати заходи щодо виключення або зниження негативних наслідків їх настання.

Подібний погляд мають І.Ю. Івченко, І.П. Миколайчук та Т.В. Цвігун. Вони розглядають механізм управління ризиками як:

сукупність методів, прийомів і заходів, що дозволяють певною мірою прогнозувати настання ризикових подій і вживати заходів до їхнього зменшення (І.Ю. Івченко [84]);

сукупність структурних елементів, методів, важелів, інструментів впливу на об'єкт управління з відповідним ресурсним забезпеченням, що формується після практичної апробації системи управління ризиками підприємства (І.П. Миколайчук [109]);

сукупність принципів, методів та важелів управління, різноманітні складові підсистеми забезпечення, взаємодія та послідовність використання яких забезпечить ефективне прийняття рішень у сфері управління ризиками підприємства (Т.В. Цвігун [164]).

Іншу наукову позицію має О. Беляєв [10], яка механізм управління ризиками характеризує як цілеспрямовану практичну діяльність, що направлена на зниження ризику, зменшення потенційних матеріальних втрат та інших негативних наслідків.

Оригінальну думку на сутнісні характеристики механізму управління ризиками надає Д.А. Штефанич, який визначає цей механізм як сукупність дій економічного, організаційного і технічного характеру, спрямованих на встановлення видів, чинників, джерел ризику, оцінку величини, розробку і реалізацію заходів щодо зменшення його рівня та запобігання можливих втрат [159].

Існує окремий погляд на сутнісні характеристики механізму управління ризиками, який представлено у вигляді сукупності механізмів мінімізації ризиків, серед яких обов'язково присутні механізми нормування, планування та бюджетування, а також управління людським капіталом. Кожний окремий механізм мінімізації ризиків має свою організацію, складається з власних процесів, регулюється за допомогою конкретних форм і методів керування, а також правових норм та правил [91].

У ході проведеного дослідження щодо суті механізму управління ризиками виявились різноманітні позиції, які характеризувалися неоднозначністю підходів, що пояснюється використанням різних методичних засад. Припускаємо, що ключовою відмінністю механізму управління ризиками доцільно вважати різні процеси за об'єктом прояву. Механізм управління ризиками має прямий вплив на об'єкт, що передбачає проведення змін якісного стану об'єкту де підґрунтям для якісних змін стають інновації. Він вважається складним багатоаспектним і багаторівневим явищем, характеризується складовими, що мають різноспрямований вплив на об'єкт управління (чи побічний вплив на об'єкт управління), та передбачає наявність двох підсистем – керованої підсистеми та керуючої підсистеми.

Підтримуємо підходи тих вчених, які зміст механізму управління ризиками, розкривають як сукупність принципів, функцій, методів та важелів, що дозволять спрогнозувати настання ризикових подій, звести ступінь впливу виявлених ризиків до мінімальних та розробити стратегії виключення або зниження негативних наслідків, у разі їх настання.

З цього приводу О. М. Полінкевич [129] підкреслює, що механізм управління − це сукупність інструментів, методів та важелів, а також групи людей, які вступають у формальні і неформальні взаємодії, які направлені на досягнення мети підприємства, що є позитивом, або ж на чинення опору різним змінам, які завжди супроводжують нововведення, що часто спостерігається в трудовому колективі будь-якого підприємства і є негативним моментом.

Фактично, механізм управління ризиками має створювати стратегічні можливості підприємствам своєчасно адаптуватися у мінливих умовах сьогодення. Варто, механізм управління ризиками розуміти як динамічну сукупність взаємопов'язаних субсистем, інструментів, методів та важелів, що дозволяють ідентифікувати, діагностувати та спрогнозувати настання ризикових подій, звести ступінь їх впливу до мінімуму та своєчасно розробити інноваційні стратегії здійснення організаційно-економічних змін щодо зниження негативних наслідків, у разі їх настання, системне застосування яких спрямоване на стійке економічне зростання підприємств при збалансованості бізнес -процесів, що сприятиме укріпленню їх конкурентних позицій й підвищенню прибутковості.

Вважаємо, що доцільність механізму управління ризиками в підприємствах відповідно до траєкторій цифровізації, з точки зору якості впливу на господарську діяльність підприємства буде проявлятися через негативні, нейтральні чи позитивні ефекти. Зазначимо, що негативні ефекти даного механізму супроводжуються значною кількістю ризиків, які є складно керованими у часі, та які спричиняють появу незапланованих втрат та збитків. Нейтральні ефекти механізму управління ризиками характеризуються невеликою кількістю ризиків, які є керованими, та наявність яких дозволяє де який час працювати як без прибутків так і без збитків. Найбільш привабливою для підприємства є механізм управління ризиками в підприємствах з генеруванням позитивних ефектів, які за наявності керованих ризиків у процесі функціонування дозволяють отримувати прибутки з урахуванням постійної реалізації заходів щодо ефективної програми управління ризиками.

Типова блок-схема ланцюга механізму управління ризиками передбачає ідентифікацію ризиків та побудову ієрархічної мультимодульної карти ризиків, діагностику управління ризиків, фільтрацію методів та інструментів щодо мінімізації чи нейтралізації ризиків, формування ризик профілю, вибір альтернатив і стратегічних орієнтирів та забезпечення постійного моніторингу і контролінгу впливу ризикоформуючих чинників для генерування стійкості, гнучкості й надійності функціонування підприємствав умовах цифровізації (рис. 1.7).

Результативність механізму управління ризиками в підприємствах залежить від композиції управління, в яку входять:

1) субсистема розвитку (мета; об'єкт управління; суб'єкт управління; завдання);

2) субсистема забезпечення (яка представлена підходами, функціями, принципами, методами, важелями та інструментами);

Рис. 1.7. Блок-схема ланцюга управління ризиками в умовах цифровізації
Примітка: складено з використанням [35, 36, 114, 144, 164, 166].

3) функціональна субсистема (включає блоки за ключовими бізнес–процесами, які знаходяться у постійній взаємодії один з одним, зокрема: операційний, фінансово-економічний, комунікаційний, технологічний. маркетинговий);

4) процесна субсистема забезпечує процес підготовки і прийняття управлінських рішень оперативного та стратегічного характеру з врахуванням негативних, нейтральних та позитивних ефектів, що допоможе керівництву оперативно реагувати (приймати управлінські рішення та розробляти стратегії управління ризиками за обраною траєкторією) на зміни зовнішнього і внутрішнього середовища відповідно до траєкторій розвитку, що в подальшому створить умови для досягнення заданого рівня конкурентоспроможності підприємства;

5) субсистема моніторингу і контролю (спостережень і перевірки процесу функціонування підприємства).

Зміст кожної із субсистем механізму управління ризиками в умовах цифровізації, та кількість блоків в кожній з них залежить від типу підприємства, сфери і масштабів діяльності, ступеня впливу чинників зовнішнього середовища і результатів діяльності підприємства відповідно до обраної траєкторії управління ризиками. Концепт побудови механізму управління ризиками підприємств в умовах цифровізації представлено на рис. 1.8. Система цілей механізму управління ризиками в підприємствах формується на основі існуючої стратегії підприємства із врахуванням можливостей та очікувань. В умовах цифрової економіки менеджмент підприємств сприяє активному впровадженню цифрових технологій у бізнес-процеси, що призводить до підвищення ефективності функціонування, зокрема, зростанню обсягів виробництва та реалізації, підвищення продуктивності праці та якості продукції (послуг), зниження собівартості, освоєння нових видів продукції (послуг), закріплення конкурентних позицій на ринку тощо.

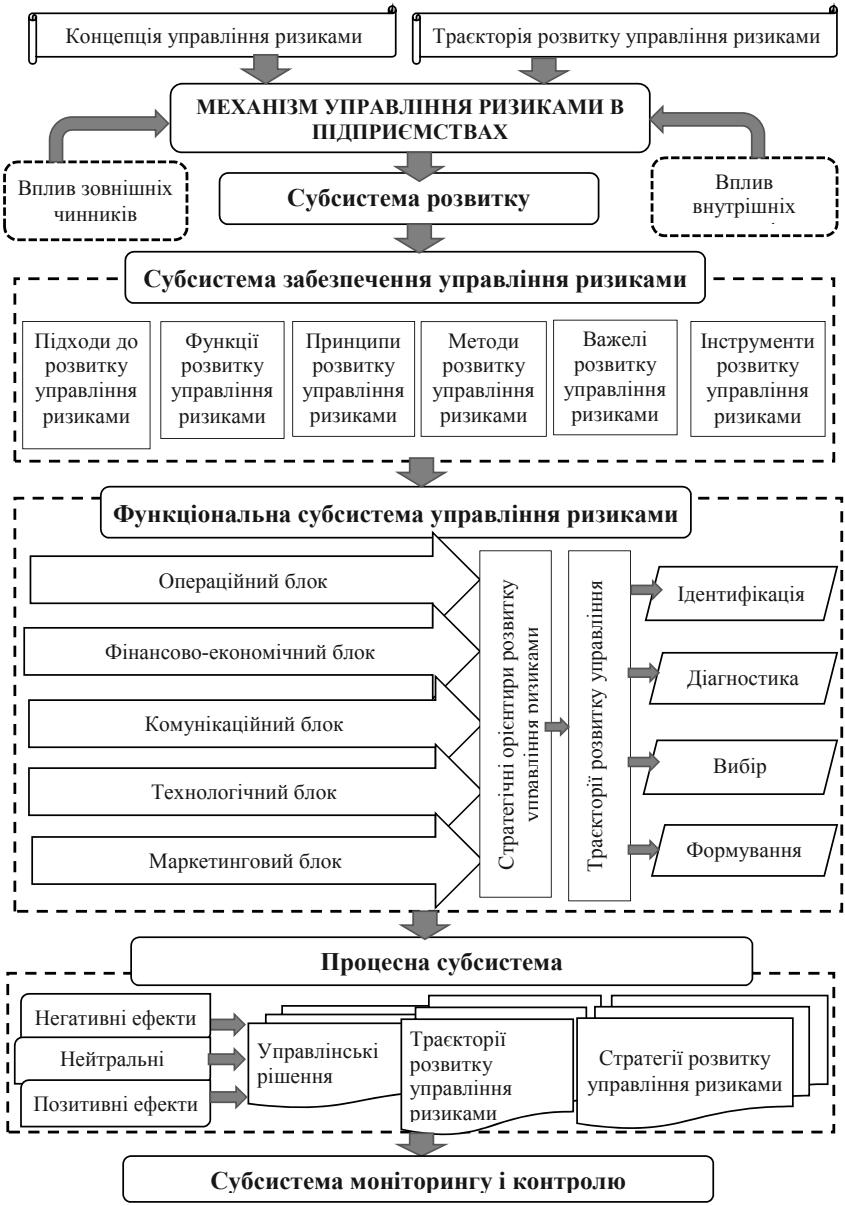


Рис. 1.8. Концепт побудови механізму управління ризиками підприємств в умовах цифровізації

Примітка: сформовано за [35, 36, 114, 144, 164, 166].

Запроваджуючи цифрові рішення, менеджмент змінює існуючі бізнес-процеси підприємств, моделі управління, переформовує комунікації, технології та організаційну структуру, ризикуючи не отримати належного результату. Крім того, не треба забувати, що проведення будь яких змін у діяльності підприємства вимагає постійного залучення фінансових ресурсів та участі у програмах інвестиційного характеру. Саме тому, процес формування та реалізації механізму управління ризиками відбувається у межах наукових підходів, функцій, принципів, важелів, методів та інструментів.

Наукові підходи до формування концепту побудови механізму управління ризиками підприємствв умовах цифровізації враховують особливості у:

системному зрізі, який забезпечує цілісність механізму як системи з визначеною структурою (цілі, ресурси, засоби, процеси, способи);

процесному зрізі, який гарантує безперервність застосування адаптаційних заходів підприємства;

ситуаційному зрізі, який забезпечує постійні дослідження зовнішнього та внутрішнього середовища з метою виявлення певних закономірностей і визначення характеру поведінки підприємства у відповідній ситуації.

Таким чином, концепт побудови механізму управління ризиками підприємств в умовах цифровізації, принциповою відмінністю якого є врахування особливостей їх функціонування у системному зрізі (забезпечує цілісність механізму як системи з визначеною структурою (цілі, ресурси, засоби, процеси, способи), процесному зрізі (гарантує безперервність застосування адаптаційних заходів підприємства) й ситуаційному зрізі (сприяє постійному моніторингу зовнішнього та внутрішнього середовища з метою виявлення закономірностей і визначення характеру поведінки підприємства у відповідній ситуації) із включенням управлінської, функціональної, процесної, контрольної субсистем й відповідних технологічних, економічно-фінансових, організаційних, інформаційних, нормативно-регламентних інструментів й важелів та методів управління ризиками.

До функцій механізму управління ризиками підприємств в умовах цифровізації відносять наступні:

організація – це процес створення, узгодження та виконання планів для менеджерів й виконавців, які об'єднуються з метою розробки і реалізації механізму управління ризиками;

планування – це процес постановки цільових настанов щодо управління ризиками та опрацюванні напрямів, якими підприємство буде досягати очікуваних результатів відповідно до завдань функціонування (тактика) і розвитку (стратегія);

мотивація – це процес впливу на менеджерів із управління ризиками та інших працівників підприємства з метою формування мотивів і стимулів персоналу до узгоджених та ефективних дій відповідно до цілей підприємства та особистих цілей;

контроль – систематичне спостереження та перевірка результатів діяльності підприємства у межах механізму управління ризиками, а також аналіз результатів, їх корегування та шляхи реалізації.

Принципами механізму управління ризиками підприємств в умовах цифровізації є наступні: системності, комплексності, гнучкості, стійкості, орієнтованості на стратегічні цілі, інтегрованості, динамізму. До основної групи принципів, слід додати ті, які доповнюють розвиток управління ризиками, зокрема, інерційності, адаптивності, безперервності, пропорційності та стабілізації [56].

Системність механізму управління ризиками завжди доповнюється його комплексністю, під якою розуміється не тільки необхідність урахування та аналізу всього спектру особливостей та чинників розвитку, але й належне поєднання застосовуваних методів здійснення змін на підприємстві.

Гнучкість механізму управління ризиками передбачає стійкість, адаптацію та пристосування підприємства до змін зовнішнього середовища, можливість коригування цільових параметрів в цілому чи окремих кількісних значень, забезпечує можливостей проведення своєчасних змін в процесі управління [162 с. 164].

Інтегрованість механізму управління ризиками із загальною системою управління підприємством, є важливим чинником, оскільки управлінські рішення, безперечно, будуть здійснювати безпосередній чи непрямий вплив на зміни підприємства. В даному випадку, рішення щодо управління ризиками поєднуються в ефективну взаємодію з усіма функціональними системами управління

Високий динамізм та безперервність механізму управління ризиками в підприємствах також є важливими принципами. Специфіка передачі інформації у просторі та часі висуває відповідні вимоги стійкості до об'єктів. У той же час, динамічна реакція на можливі відхилення в ході впровадження змін на підприємстві під впливом внутрішніх та зовнішніх чинників означає гнучкість системи управління.

Інерція механізму управління ризиками проявляється в продовженні змін потенціалу системи на деякий час навіть після закінчення впливу змін у зовнішньому та внутрішньому середовищі. У свою чергу швидкість змін у механізмі управління ризиками залежить від інтенсивності поступу підприємства та його мети і стратегій. Принцип стабілізації вказує на прагнення системи стабілізувати зміни щодо управління ризиками у період зростання.

До важелів механізму управління ризиками в підприємствах відносять: економічні; правові; техніко-технологічні; інформаційно-технологічні, соціальні, управлінські; організаційні.

Вагоме значення у механізмі управління ризиком підприємства в умовах цифровізації відіграє вибір і використання адекватних методів управління ризиком. Слід підтримати наукові позиції дослідників [65], які до ключових методів управління ризиком відносять: „запобігання (уникнення), відхилення, зниження, збереження (прийняття), передача, поділ відповідальності, використання, ігнорування" [60] (рис. 1.9).

Рис. 1.9. Методи управління ризиком
Примітка: систематизовано на основі [35, 36, 40, 51, 114, 144, 154, 164, 166, 169]

При відборі та використанні методів управління ризиками, варто зважати на „особливості функціонування самого підприємства (організаційний дизайн, обсяги діяльності, форму власності, ступінь діджиталізації, вплив ризикоформуючих чинників тощо)" [60].

Визначаючи конкретні методи управління ризиком, слід зважати на наступні чинники:

складність операційних бізнес-процесів щодо генерування продуктів чи послуг (функції та алгоритми;

адаптивність організаційного дизайну;

значний неформальний вплив на персонал;

великий обсяг інформаційних потоків;

обмеженість часу та ресурсів);

технологічні вимоги (необхідність чіткого дотримання технологічних вимог;

постійна технологічна модернізація та цифровізація бізнес-процесів;

вимоги до якості продуктів та послуг);

клієнтське та зовнішнє середовище (кількість мереж, вузлів і клієнтів;

ефективність процедур взаємодії із клієнтами;

компетентність клієнтів та рівень їх вимог;

пріоритети, виклики та вплив зовнішнього середовища;

часова обмеженість для відповідей на запити клієнтів;

необхідність трансформацій процедур, взаємозв'язки із партнерами, постачальниками, субпідрядниками);

середовище функціонування підприємства (розклади, їх незмінність, хиткість та гнучкість;

рівень компетенцій та стабільності кадрів;

реорганізація офісів, філій та процедур;

оцінка часових, ресурсних та організаційних контурів).

Тобто, для визначення конкретних методів управління ризиком, слід зважати на: складність алгоритмів операційних бізнес-процесів; адаптивність організаційного дизайну; обсяг інформаційних потоків; технологічні вимоги та компоненти й рівень діджиталізації; кількість мереж, вузлів, партнерів і клієнтів; ефективність комунікаційних ланцюгів взаємодії; обмеження й виклики та пріоритети й можливості; хиткість і гнучкість зовнішнього середовища; рівень компетенцій кадрів; параметри часових, ресурсних та організаційних контурів.

Вважаємо за необхідне виділити ряд інструментів механізму управління ризиками в підприємствах:

технологічні інструменти для підвищення ефективності (компоненти цифровізації, програмні продукти);

фінансові інструменти (реструктуризації, фінансового контролінгу);

управлінські інструменти, що сприяють досягненню цілей та ефективному розвитку підприємства (проекти, плани, стратегії, методики);

кадрові інструменти, що сприяють розвитку кадрового потенціалу (обмін досвідом, перекваліфікація, навчання);

нормативно-регламентні інструменти (податкові ставки, субсидії та пільги, стандарти якості, організаційні й комунікаційні регламенти тощо).

В даних обставинах, всі заходи, що з'являться у ході реалізації концепту побудови механізму управління ризиками в підприємствах будуть спрямовані на задоволення економічних інтересів власників окремого підприємства та його працівників з метою формування максимального потенціалу підприємства в умовах невизначеності та ризику.

Однак є випадки прояву інерційності в діяльності підприємств в умовах цифровізації, які проявляється у використанні застарілого обладнання, знань, організаційних структур, норм, правил тощо. Тому є необхідним організувати на підприємствах систему моніторингу та контроля, що дозволить оперативно вирішувати не тільки поточні проблеми, але й задачі стратегічної спрямованості. У цьому сенсі, механізм управління ризиками, допоможе приймати рішення щодо оптимізації співвідношення між прибутковістю та ризиком для максимізації прибутку та вартості підприємства як нині, так і на стратегічну перспективу.

Таким чином, механізм управління ризиками необхідно розуміти як динамічну сукупність взаємопов'язаних субсистем, інструментів, методів та

важелів, що дозволяють ідентифікувати, діагностувати та спрогнозувати настання ризикових подій, звести ступінь їх впливу до мінімуму та своєчасно розробити інноваційні стратегії здійснення організаційно-економічних змін щодо зниження негативних наслідків, у разі їх настання, системне застосування яких спрямоване на стійке економічне зростання підприємств при збалансованості бізнес -процесів, що сприятиме укріпленню їх конкурентних позицій й підвищенню прибутковості.

А, реалізація концепту побудови механізму управління ризиками в підприємствах, вагомо впливатиме на ефективність функціонування підприємств відповідно до його мети та обраної стратегії поступу, що зорієнтує менеджерів та працівників підприємства на активну й цілеспрямовану діяльність направлену на підвищення їх конкурентних можливостей й зміцнення конкурентних позицій на ринку та зростання прибутків у довгостроковій перспективі, допоможе приймати рішення щодо оптимізації співвідношення між прибутковістю та ризиком для максимізації прибутку та вартості телекомунікаційного підприємства як нині, так і на стратегічну перспективу. Змістове наповнення і структура кожної із субсистем механізму розвитком управління ризиками залежить від типу підприємства, сфери, масштабів і результатів його діяльності, ступеня впливу чинників зовнішнього і внутрішнього середовища, що надасть можливість удосконалювати проектування такого механізму із заданими властивостями, що допоможе підприємству більш досконалого перейти з одного стану до іншого.

Для визначення конкретних методів управління ризиком, слід зважати на: складність алгоритмів операційних бізнес-процесів; адаптивність організаційного дизайну; обсяг інформаційних потоків; технологічні вимоги та компоненти й рівень цифровізації; кількість мереж, вузлів, партнерів і клієнтів; ефективність комунікаційних ланцюгів взаємодії; обмеження й виклики та пріоритети й можливості; хиткість і гнучкість зовнішнього середовища; рівень компетенцій кадрів; параметри часових, ресурсних та організаційних контурів.

Контрольні питання для самодіагностики по тематиці 1 модуля

1. Розкрийте поняття „ризик”.
2. Назвіть причини виникнення ризикової ситуації.
3. Дайте визначення економічного ризику.
4. Як пов’язані поняття „ризик” і „невизначеність”?
5. Які виділяють види чинників ризику?
6. Назвіть основні елементи ризику.
7. У чому полягає інноваційна функція ризику?
8. Розкрийте поняття „класифікація ризиків”.
9. Назвіть головні принципи класифікації ризиків підприємства.
10. Як класифікують ризики за наслідками?
11. Як класифікують ризики за характером діяльності?
12. Як класифікують ризики за ступенем непередбачуваності?
13. Назвіть специфічні види ризики телекомунікаційних підприємств.
14. Розкрийте поняття „управління ризиками”.
15. Назвіть головні завдання управління ризиками.
16. Що належить до головних функцій управління ризиками?
17. Із яких етапів складається процес управління ризиками?
18. Що належить до головних функцій менеджера з ризику?
19. Назвіть основні методи управління ризиками.
20. Як ви розумієте сутність методу диверсифікація ризику?
21. У чому полягає сутність методу ухиляння від ризику?
22. Що становить метод лімітування ризику?
23. У чому полягає метод компенсації ризиків шляхом створення системи резервів?
24. Охарактеризуйте особливості управління ризиками в проектах цифровізації підприємств.
25. Назвіть складові механізму управління ризиками в підприємствах.
26. Перерахуйте принципи побудови механізму управління ризиками в підприємствах.

МОДУЛЬ 2
ПРАКТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ

2.1. Методичні підходи до діагностики управління ризиками підприємств.

Функціонування та поступ сучасного економічного простору відбувається за умов систематичної та перманентно зростаючої невизначеності. Це супроводжується ускладненням причино-наслідкових та функціональних зв'язків, турбулентністю економічної реальності та генеруванням загроз і негативних подій у діяльності підприємств. Саме тому важливим ключовим напрямом сучасної економічної науки вважається діагностика управління ризиком й впровадження різноманітних методичних підходів та інструментів щодо активізації та ефективності процесу управління ризиками з метою їх нейтралізації та мінімізації.

Термін „діагностика", запозичений з медицини, де слово „діагноз" означає розпізнавання, визначення, тобто процес дослідження об'єкту діагностики задля одержання результату (діагнозу) − висновку про його стан. Загалом, діагностика розглядається з різних точок зору і трактування її не є однозначним.

Здебільшого, вчені-економісти трактують діагностику як: спосіб встановлення характеру порушень, виявлення кризових явищ та процесів, банкрутства, рівня фінансової та економічної безпеки [45]; напрям економічного аналізу, що дозволяє виявити характер порушення нормального ходу економічних процесів на підприємстві [97]; дослідження, що дозволяє не тільки всебічно оцінювати стан об'єкта в умовах неповної інформації, але й виявляти проблеми його функціонування, окреслювати шляхи їх вирішення, враховуючи коливання параметрів системи [102]. Цікаві пропозиції розроблено щодо системи оцінювання ризиків підприємства (додаток) та комплексної оцінки ризиків підприємства та прийняття управлінських рішень на основі результатів оцінки (додаток).

В.В. Лук'янова стверджує: „сучасним управлінським інструментарієм є діагностика – процес розпізнавання і виявлення на основі визначених ознак (ключових оціночних показників, вивчення окремих результатів, неповної інформації) у функціонуванні об'єкта з метою оцінки наявних тенденцій і виявлення можливих перспектив його розвитку та аналізу варіантів найкращого вирішення виявлених проблем" [101].

Залежно від масштабів, мети і напрямів діагностики, а також доступної інформації та ресурсних можливостей, доцільно здійснювати: „діагностичний експрес-аналіз (найпростіша і найперша діагностична процедура), комплексний діагностичний аналіз (найскладніший вид діагностики), діагностичний аналіз функціональних напрямів (зокрема, діагностика ризиків виробництва, пов'язаних з високо ризикованим природнім середовищем),

діагностичний аналіз прикладних питань, діагностику проблемних зон, діагностику в проекті організаційного розвитку" [5].

Діагностика управління ризиками підприємств – це структурований процес оцінки поточного рівня організації управління ризиками на підприємстві та досягнутого ним рівня економічної стійкості з урахуванням структурованих чинників ризику, що має на меті виявлення стратегічних пріоритетів і перспектив подальшого управління ризиками в нових реаліях цифровізації.

Необхідність діагностики управління ризиками підприємства для виявлення проблемних зон, не викликає сумнівів та усвідомлюється усіма дослідниками. Проте, вимоги до змісту, алгоритму її проведення, перелік об'єктів діагностики, системи показників та методології узагальнення отриманих результатів перебувають у стадії вдосконалення та неоднозначно трактуються науковцями.

На рисунку 2.1, продемонстровано загальний алгоритм діагностики управління ризиками підприємства.

1.

Рис. 2.1. Загальний алгоритм діагностики управління ризиками підприємства
Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

Сам процес діагностики управління ризиками підприємства переважно розглядається як система елементів, призначених для перетворення вихідної інформації про стан об'єкта управління шляхом проведення діагностичних процедур на можливі рекомендації щодо зменшення негативних впливів і поліпшення (відновлення) стану об'єкта. Фактично, діагностика управління ризиками підприємства має враховувати обмеженість управлінського впливу та параметри стійкості самого підприємства, тобто варто виділити три напрями діагностики управління ризиками підприємства на різних ієрархічних рівнях (рис. 2.2).

Рис. 2.2. Діагностика управління ризиками підприємства на різних ієрархічних рівнях
Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

Переконуємось, що вирішення проблеми діагностики управління ризиками підприємств відноситься до складних, багатокритеріальних завдань, оскільки має передбачати:

визначення тенденцій управління ризиками підприємств в Україні та побудова на цій основі багатовекторних концептуальних схем і моделей управління ризиками на усіх ієрархічних управлінських рівнях;

обґрунтування ключових чинників, які впливають на управління ризиками підприємств на мікрорівні;

діагностика ефективності управління ризиками на підприємствах з урахуванням існуючого рівня цифровізації, організації управління ризиками та рівня економічної стійкості підприємств.

Ґрунтовні рекомендації щодо кількісної діагностики управління ризиками наводять В. В. Вітлінський та Г. І. Великоіваненко: „вимірювальними властивостями економічних систем повинні бути характеристики структури, стану, динаміки чи поведінки цих систем та зовнішнього середовища, котрі дають змогу в умовах невизначеності та конфлікту віднайти й деталізувати за потенційними наслідками можливі майбутні стани чи траєкторії (їх множину) поведінки певних економічних об'єктів, можливі відхилення від цілей, можливі збитки, невикористані можливості" [22 с.16]. Слід вказати, що визначення рівня стійкості підприємств і здійснення інтегральної оцінки рівня окремих її складових вже застосовується вітчизняними ученими в процесі діагностики управління ризиками. Так, Савченко М. В. і Солоненко Ю. В. розробляючи науково-методичний підхід до управління ризиками підприємств підкреслюють, що необхідно в першу чергу визначити важливий результат функціонування підприємств, а саме стійкість [143]. Автори вказують, що стійкість є зовнішнім проявом внутрішньої структури об'єкта. А для того щоб підвищити його стійкість до впливу різних чинників ризику, необхідно, перш за все, удосконалювати сам об'єкт. Погоджуючись з ученими в плані того, що для забезпечення стійкості підприємства керівництво повинно прагнути мінімізувати ризики його діяльності, вважаємо за доцільне відштовхуватись

саме від досягнутої економічної стійкості. Високий рівень економічної стійкості є головним проявом ефективного управління ризиками на підприємстві. Оцінку рівня економічної стійкості підприємств, необхідно проводити на основі визначених ключових макро-, мезо- і мікро чинників, які впливають на розвиток управління ризиками. Найбільш релевантною для підприємств, є 4-ох елемента система показників (додаток). Іншим аспектом, який повинен бути врахований при діагностиці управління ризиками підприємств є рівень організації управління ризиками на підприємстві.

Організаційним аспектам управління ризиками присвячені дослідження Сосновської О.О., Ріщук Л.І., Гусєвої О.Ю. та інших. Означені роботи розкривають групи оціночних критеріїв для визначення ефективності управління ризиками [81], виокремлюють бізнес-процеси управління ризиками і впорядковують компоненти управління ризиками за провідними методологіями і стандартами (наприклад, COSO ERM) [195], визначають та ув'язують організаційні центри відповідальності з етапами управління ризиками на підприємстві [146] (додатки).

Отже, у сучасних умовах ключовими вважаються два імперативи діагностики ефективності управління ризиками (рис. 2.3).

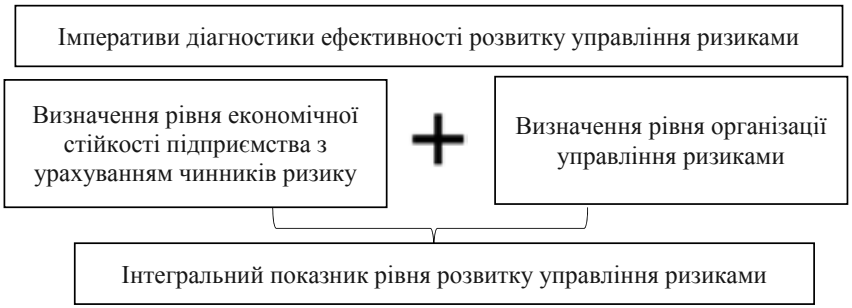


Рис. 2.3. Імперативи діагностики ефективності управління ризиками
Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

Узагальнення означених досліджень дозволило визначити підходи до організації управління ризиками підприємства (табл. 2.1).

На основі визначених підходів до організації управління ризиками підприємств обґрунтовуються критерії оцінки рівня управління ними і відповідні показники для оцінки (табл. 2.2). *Примітка. Наближення кожного із запропонованих коефіцієнтів до 1 свідчить про високий рівень організації управління ризиками на підприємстві. Далі, в процесі обробки даних розраховуються таксономічні показники рівня розвитку підприємства, що узагальнено характеризують напрями та масштаб перетворень, пов'язаних з управлінням ризиками.

Таблиця 2.1

Підходи до організації управління ризиками підприємств

№	Підхід	Характеристика (складові елементи підходу)	Переваги	Недоліки
1	Реактивний	1.Система організації, планування і контроля ризиків побудована на виконанні формальних вимог Українського законодавства. 2.Інструменти і методи управління ризиками є типовими і не адаптованими до специфіки підприємства. 3.Не застосовуються сучасні програмні рішення для оцінки і прогнозування ризиків. 4.В організаційній структурі немає чітко визначених організаційних підрозділів (центрів), відповідальних за управління ризиками. 5.Корпоративна культура не орієнтована на цінності, пов'язані з розвитком схильностей до ризику та розумінням значущості управління ризиками.	- мінімальні витрати на організацію управління ризиками; - при достатньому потенціалі зростання тарифів на телекомунікаційні послуги усі втрати від реалізації ризику компенсуються за рахунок додаткового прибутку.	- невизначеність рівня загроз; - невідслідковування динаміки ризикового потоку; - недостатня фіксація ризикових подій; - максимізація витрат на компенсацію збитків і страхування ризиків.
2	Стандартний	1. Система організації, планування і контроля ризиків є достатньо зрілою, проте недостатньою для ефективної протидії складним ризикам; враховано імплементовані в Україні міжнародні стандарти ISO 31000:2018 та COSO; 2. Інструменти і методи управління ризиками адаптовані до специфіки підприємства; більше половини (від 50 %) ризиків розподіляються і компенсуються до появи деструктивних чинників. 3. Частково застосовуються сучасні програмні рішення для оцінки і прогнозування ризиків. 4. В організаційній структурі або на основі	- компенсація витрат на організацію управління ризиками відбувається за рахунок зростання доходів, що відбувається завдяки ідентифікації і нейтралізації більшості ризиків;	- середній (недостатньо упереджуваний) рівень визначення загроз; - несистематичний («час від часу») контроль ризиків за умов передачі функцій управління ризиками на аутсорсинг.

		аутсорсингу сформовані підрозділи (центри), відповідальні за управління ризиками. 5.Корпоративна культура розвиває і підтримує цінності, пов'язані з схильностями до ризику та управління ним.		
3	Прогресивний	1.Система організації, планування і контроля ризиків є динамічною та ефективно протидіє складним ризикам; враховано імплементовані в Україні міжнародні стандарти ISO 31000:2018, COSO та FERMA; всі функції управління ризиками збалансовані; 2. Інструменти і методи управління ризиками адаптовані до специфіки підприємства; більша частина (від 75 %) ризиків розподіляються і компенсуються до появи деструктивних чинників. 3. Застосовуються програмні рішення останніх поколінь для оцінки і прогнозування ризиків. 4. В організаційній структурі сформовані підрозділи (центри), відповідальні за управління ризиками. 5.Корпоративна культура формує максимальну залученість усіх працівників у розумінні значущості управління ризиками.	- ефективність стратегічного та оперативного управління підприємством за рахунок збалансованості усіх функцій управління ризиками; - створення максимально сприятливих умов для безперервності і захищеності ключових бізнес-процесів.	- висока витрато ємність створення і підтримки прогресивної системи організації, планування і контроля ризиків.

Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

Таблиця 2.2

Обґрунтування критеріїв і показників оцінки рівня організації управління ризиками телекомунікаційного підприємства

Складові елементи підходу	Критерій оцінки	Відповідний показник для оцінки та алгоритм розрахунку
Система організації, планування і контроля ризиків	Рівень збалансованості усіх елементів системи управління ризиками	Коефіцієнт нейтралізації складних ризиків (*Кнср*) $$К_{нср} = \frac{РИЗ_{нс}}{РИЗ_{зс}}$$ де $РИЗ_{нс}$ – кількість нейтралізованих складних ризиків за звітний період; $РИЗ_{зс}$ – загальна кількість ідентифікованих складних ризиків за звітний період.
Інструменти і методи управління ризиками	Рівень адаптивності (інноваційності, гнучкості) інструментів управління ризиками	Коефіцієнт адаптації інструментів управління ризиками до специфіки підприємства (*Каір*) $$К_{аір} = \frac{ІНР_{ад}}{ІНР_{ад} + ІНР_{тип}}$$ де $ІНР_{ад}$ – кількість адаптованих (інноваційних, гнучких) інструментів управління ризиками; $ІНР_{тип}$ – кількість типових інструментів управління ризиками
Програмні рішення, що застосовуються для оцінки і прогнозування ризиків	Рівень застосування сучасних програмних рішень, для оцінки і прогнозування ризиків	Коефіцієнт автоматизації (цифровізації) оцінки ризиків (*Каор*) $$К_{аор} = \frac{РИЗ_{авт}}{РИЗ_{заг}}$$ де $РИЗ_{авт}$ – кількість автоматизованих сучасними програмними рішеннями етапів оцінки ризиків; $РИЗ_{зс}$ – загальна кількість ідентифікованих етапів оцінки ризиків.
Наявність організаційних центрів, відповідальних за управління ризиками	Рівень охоплення функцій управління ризиками організаційними підрозділами	Коефіцієнт організаційної відповідальності за управління ризиками (*Корв*) $$К_{орв} = \frac{ФУР_{орв} + ФУР_{аут}}{ФУР_{заг}}$$ де $ФУР_{орв}$ – кількість функцій управління ризиками закріплених за підрозділами підприємства; $ФУР_{аут}$ - кількість функцій управління ризиками відданих на аутсорсинг; $ФУР_{заг}$ – загальна кількість встановлених функцій управління ризиками
Спрямованість цінностей корпоративної культури на розвиток управління ризиками	Рівень підтримки працівниками культури «проактивного управління ризиками»	Коефіцієнт розвитку культури проактивного управління ризиками (*Кпур*) $$К_{пур} = \frac{ПР_{пур}}{ПР_{заг}}$$ де $ПР_{пур}$ – кількість працівників, які підтримують культуру проактивного управління змінами та відповідні цінності; $ПР_{заг}$ – загальна кількість працівників підприємства

Примітка: сформовано за [5, 34, 91, 98, 99, 101, 154, 160].

На першому етапі досліджень відбувається побудова матриці розвитку окремих показників управління ризиками у часі.

$$X_{ti} = \begin{bmatrix} x_{11}... & x_{1i}... & x_{1m} \\ x_{t1}... & x_{ti}... & x_{tm} \\ x_{T1}... & x_{Ti}... & X_{Tm} \end{bmatrix} \quad (2.1)$$

де $t = 1,...,T$ – номер часового етапу;

$i = 1,...,m$ – номер показника збалансованої системи для підприємства, що розглядається.

Слід зазначити, що показники, які включено до матриці, є неоднорідними, оскільки описують різні властивості досліджуваного підприємства і характеризуються різними одиницями виміру.

Отже, в процесі проведення таксономічного аналізу виконується процедура стандартизації показників, яка призводить не тільки до елімінування одиниць виміру, а й до вирівнювання значень показників.

Під час стандартизації показників можуть вводитись коефіцієнти ієрархії, що розділяють показники за ступенем їх вагомості. Стандартизація показників з урахуванням їх змін у часі здійснюється за наступними правилами.

$$Z_{ti} = \frac{x_{ti} - \overline{x_i}}{S_i} \quad (2.2)$$

де Z_{ti} – стандартизоване значення елемента матриці x_{ti};

$\overline{x_i}$ – середнє значення показника x_i у підмножині $t = 1,...,T$;

S_i – стандартне відхилення показника x_i.

$$\overline{x_i} = \frac{1}{T}\sum_{t=1}^{T} x_{ti} \quad (2.3)$$

$$S_i = \left[\frac{1}{T}\sum_{t=1}^{T}(x_{ti} - \overline{x_i})^2\right]^{1/2} \quad (2.4)$$

Стандартизована матриця спостережень має такий вигляд.

$$Z_{ti} = \begin{bmatrix} Z_{11}... & Z_{1i}... & Z_{1m} \\ Z_{t1}... & Z_{ti}... & Z_{tm} \\ Z_{T1}... & Z_{Ti}... & Z_{Tm} \end{bmatrix} \quad (2.5)$$

Для визначення напряму подальшого управління ризиками доцільно використовувати таксономічний показник рівня розвитку, запропонований З. Хельвигом. Показник рівня розвитку використовується для встановлення характеру та напряму управління ризиками для підвищення економічної ефективності підприємства. В процесі оцінки рівня управління ризиками підприємства множина обраних показників піддається диференціації в залежності від характеру впливу кожного з них на рівень розвитку досліджуваного об'єкту. Показники, які спричиняють позитивний, стимулюючий вплив на рівень розвитку об'єкту, відносять до групи стимуляторів. Відповідно, показники, що мають негативний вплив, – до групи дестимуляторів.

На основі врахування означеного впливу виділяється еталон розвитку об'єкту, який являє собою точку P_0 з координатами $Z_{01,}Z_{02},...,Z_{0s},...Z_{0m}$,

$$Z_{0s} = \max_r Z_{rs,} \quad \text{якщо } s \in I \tag{2.6}$$

$$Z_{0s} = \min_r Z_{rs,} \quad \text{якщо } s \notin I \tag{2.7}$$

де I – множина стимуляторів;

Z_{rs} – стандартизоване значення показника s для часового періоду r.

Показник рівня розвитку розраховується у такий спосіб.

$$d_t = 1 - \frac{C_{t0}}{C_0} \tag{2.8}$$

де d_t – таксономічний показник рівня розвитку підприємства для часового періоду t ($t = 1,...,T$);

C_{t0} – відстань кожного показника у різні періоди t від його максимального (еталонного) значення.

$$C_0 = \overline{C_0} + 2S_0 \tag{2.9}$$

де $\overline{C_0}$ – середнє значення відстані C_{t0}.

$$\overline{C_0} = \frac{1}{T}\sum_{t=1}^{T} C_{t0} \tag{2.10}$$

$$C_{t0} = \left[\sum_{s=1}^{m}(Z_{ts} - Z_{0s})^2\right]^{1/2} \tag{2.11}$$

$$S_o = \left[\frac{1}{T}\sum_{t=1}^{T}(c_{t0} - \overline{c_0})^2\right]^{1/2} \tag{2.12}$$

Розраховані у такий спосіб показники рівня економічної стійкості та рівня організації управління ризиками описують динаміку змін досліджуваних наборів показників і узагальнено ефективність управління ризиками в підприємстві.

$$d_t = d_{1,},...,d_t,...d_T \tag{2.13}$$

Інтерпретуються ці показники таким чином: чим більш наближеним є значення показника d_t до одиниці, тим більш економічно стійким і ефективнішим в плані організації управління ризиками є підприємство у різні періоди часу і напрям (фокус) змін у такому випадку формулюється як: „Забезпечення стійкого розвитку підприємства на основі постійних покращень та удосконалень вже досягнутого високого (проактивного) рівня управління ризиками". Значення показника d_t далеке від одиниці засвідчує низький рівень управління ризиками (тобто реактивний, який не відповідає вимогам сьогодення) і, відповідно, вимагає принципового перегляду організаційних та економічних складових управління ризиками.

Водночас, для превентивного гальмування розгортання ризикових процесів та явищ в підприємствах необхідно виявляти, ідентифікувати та оцінювати ризики. Доцільно це здійснювати з використанням конкретизації ієрархічної мультимодульної карти ризиків, що дасть змогу генерувати стратегічні конкурентні перспективи, забезпечити економічну сталість функціонування підприємств до агресивних впливів зовнішнього оточення. На підтримку цієї позиції Р. Каплан і Д. Нортон [186 с.169], зазначають, що „для того, щоб послідовно захищати підприємство від ризиків, необхідно чітко їх описати у форматі, що буде однозначно зрозумілим усім.

Один із таких способів опису є картографування". Артищук І.В. [4], Ріщук Л.І. [140], Супрун А.А. [154] вважають, що доцільно використовувати карту ризиків, в якій надається графічний опис та характеристика ризиків підприємства, переважно ризики розміщують у матричній таблиці, на якій наочно демонструють вагомість впливу чи значення ризику та імовірність, інтенсивність чи частоту його настання (рис. 2.4).

Існують різні способи формування ієрархічної мультимодульної карти ризиків та її використання.

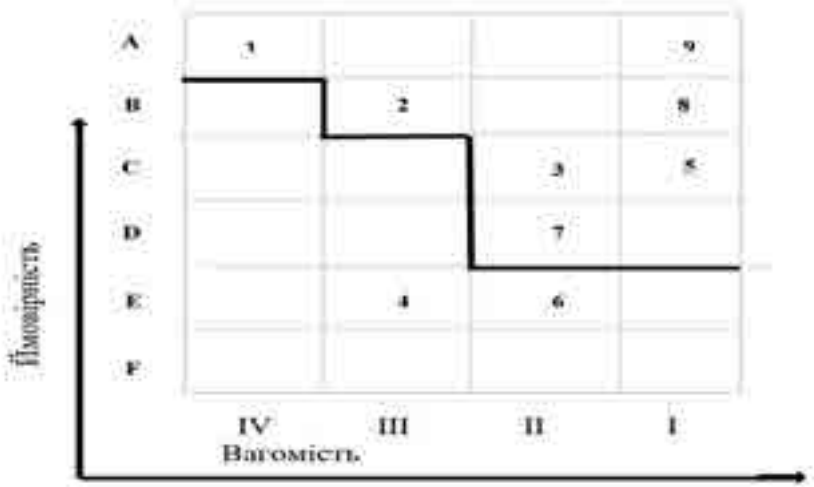


Рис. 2.4. Приклад ієрархічної мультимодульної карти ризиків
Примітка: Складено з використанням [4, 140, 154], *1- технологічні ризики; 2- ризики діджиталізації; 3- виробничі ризики; 4 – підприємницькі ризики; 5 – кібер-ризики; 6 - інвестиційні ризики; 7 – нормативно-регламентні ризики; 8 – технологічні ризики; 9 – організаційно-комунікаційні ризики.*

Цей принцип формування ієрархічної мультимодульної карти ризиків та її використання не вважається повністю оптимальним, однак він допомагає формувати оптимальну ризикостійкість.

Ієрархічна мультимодульна карта ризиків, дозволяє наочно продемонструвати місце, роль і значення конкретного ризику відносно

діяльності підприємства та формує передумови щодо ефективного управління ним. Загалом, мультимодульна карта ризиків сприяє систематизації ризиків підприємства за пріоритетами, вагомістю, інтенсивністю та дає змогу якісно їх ідентифікувати. Інструментами при формуванні карти ризиків можуть бути: інтерв'ю, анкетування, формалізовані і неформалізовані опитувальники, спеціально зібрана інформація, дослідження тенденцій галузі, економічний моніторинг звітів підприємства тощо. Важливими завданнями формування мультимодульної карти ризиків вважаються: виявлення критичних чи катастрофічних ризиків, визначення контурів управлінського впливу та ресурсних можливостей для цього, сприяння формуванню команди, окресленню часових горизонтів і пріоритетів, розробці альтернативних сценаріїв, прогнозів та плану заходів і моделюванню. Опираючись на узагальнення наявних методичних підходів щодо діагностики управління ризиками підприємства, як засобу виявлення та ідентифікації й оцінки кризових явищ та процесів, слід використати організаційний контур діагностики управління ризиками підприємств (рис. 2.5).

Таким чином, для ефективного функціонування підприємства необхідно постійно розглядати ризикоформуючі чинники, вчасно їх ідентифікувати та здійснювати комплексну діагностику ризиків, що витікають зі специфіки діяльності підприємства та на підґрунті отриманої діагностики ухвалювати рішення щодо оптимального пакету варіантів управління ризиками.

Для превентивного гальмування розгортання ризикових процесів та явищ в підприємствах необхідно виявляти, ідентифікувати та оцінювати ризики за допомогою здійснення діагностики та побудови ієрархічної мультимодульної карти ризиків

Діагностика управління ризиками підприємств – це структурований процес виміру й аналізу досягнутого рівня управління ризиками з урахуванням економічної стійкості підприємства з метою виявлення можливостей та визначення стратегічних орієнтирів і перспектив подальшого управління ризиками в умовах цифрової економіки, що являється складним багатокритеріальним завданням. Слід використовувати організаційний контур й релевантність його здійснення з використанням ключових макро-, мезо- і мікро чинників, які впливають на розвиток управління ризиками на основі 4-ох елементної системи показників та розрахунків таксономічних індикаторів й критеріальної оцінки рівня розвитку з відповідними оціночними індексами, що дає змогу окреслити динаміку змін досліджуваних наборів показників, побудувати ієрархічну мультимодульну карту ризиків та визначити ефективність управління ризиками в підприємстві.

Побудова й конкретизація ієрархічної мультимодульної карти ризиків, з використанням інтерв'ю, анкетування, формалізованих і неформалізованих опитувальників, спеціально зібраної інформації, досліджень тенденцій галузі, економічного моніторингу звітів підприємства тощо, дозволяє наочно продемонструвати місце, роль і значення конкретного ризику,

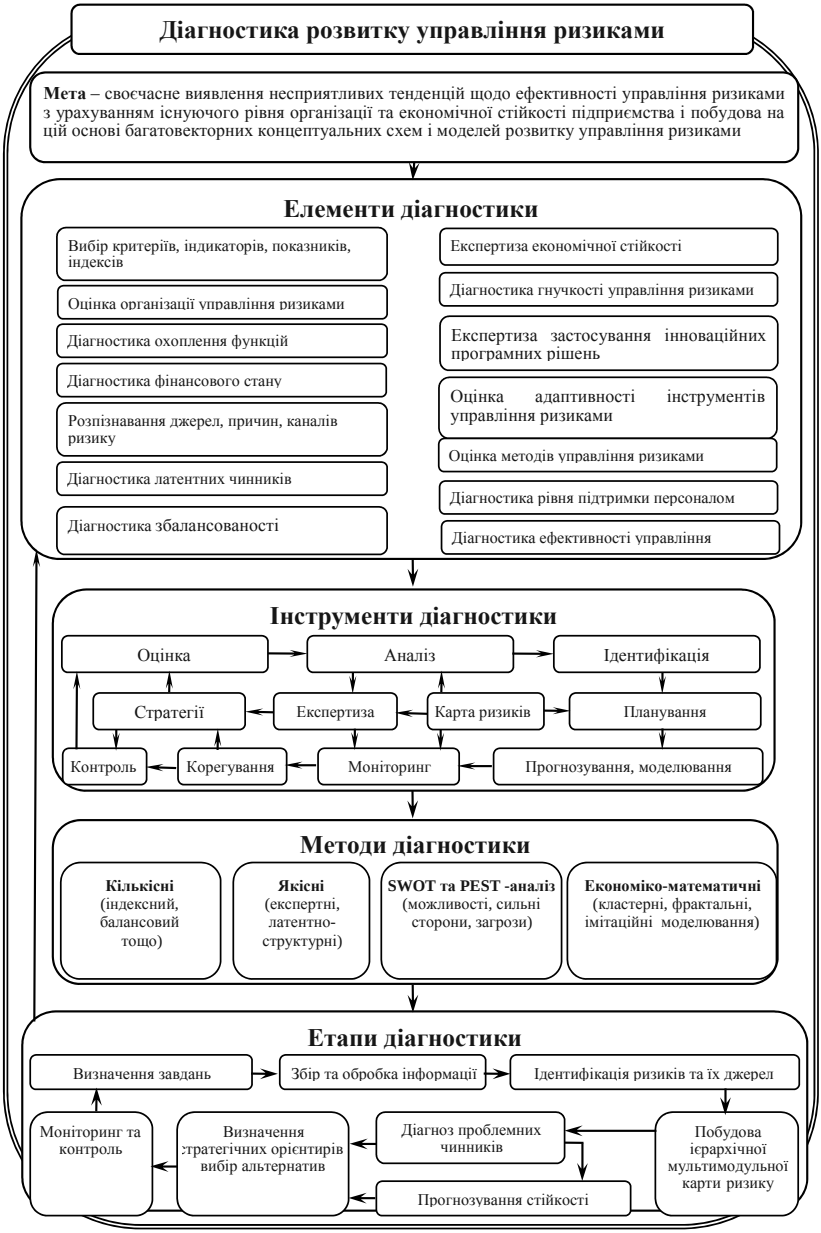


Рис. 2.5. Організаційний контур діагностики управління ризиками підприємств
Примітка: сформовано за [5, 34, 91, 99, 154, 160].

сприяє якісній ідентифікації й систематизації ризиків підприємства за пріоритетами, вагомістю, інтенсивністю, виявленню критичних чи катастрофічних ризиків, визначенню контурів управлінського впливу та ресурсних можливостей, окресленню часових горизонтів і пріоритетів, розробці альтернативних сценаріїв, прогнозів та плану заходів і моделюванню, що дасть змогу мати своєчасну об'єктивну ідентифікацію про стан ризикозахищенності підприємств та моделювати альтернативні траєкторії розвитку для досягнення бажаних результатів, організувати відповідну команду, генерувати стратегічні конкурентні переваги й забезпечити економічну сталість функціонування підприємств до агресивних впливів зовнішнього оточення.

Треба відзначити, що будь-яке сучасне підприємство використовує у своїй діяльності інформаційно-комунікаційні послуги. При цьому це стосується багатьох сфер: охорони здоров'я, освіти, сільського господарства, торгівлі, фінансів, управління комунальним господарством.

Інформаційно-комунікаційні послуги виступають необхідним посередником обслуговування таких важливих сфер життєдіяльності, як банківська діяльність, охорона та безпека, моніторинг транспорту та логістика, промисловість, сільське господарство, енергетика тощо.

Згідно плану заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки наша країна впроваджує наступні напрями цифровізації які безпосередньо стосуються підприємств [92]:

нормативно-правове та організаційно-методичне забезпечення розвитку;

розвиток пріоритетних напрямів цифровізації і послуг, зокрема;

виробництво і розвиток експорту цифрових технологій;

цифровізація пріоритетних та соціально-орієнтованих сфер життєдіяльності;

розвиток цифрових компетенцій, грамотності та навичок громадян;

розвиток цифрових інфраструктур взаємодії держава-бізнес-населення.

Водночас, зауважимо, що управління ризиками в підприємствах, пов'язаний з ресурсними обмеженнями, тобто важливою умовою є отримання прибутків і ефективності їх діяльності, оскільки управління ризиками істотно залежить від кількості та обсягів наявних ресурсів – інтелектуальних, енергетичних, матеріальних, фінансових та інформаційних.

Управління ризиками в підприємствах у високо конкурентному середовищі залежить від гостроти конкуренції та вимог споживачів до якості і вартості послуг, які надаються. Тому, основними індикативними параметрами управління ризиками повинні бути мобільність, гнучкість та унікальність продукту, а стратегії управління ризиками мають враховувати основні вимоги внутрішнього та глобального ринків. Управління ризиками, внаслідок глобалізації ринків, має враховувати, також, композицію побудови інфраструктури та комунікацій, логістичних ланцюгів та необхідності формування єдиних інформаційно-комунікативних мереж автоматизації та диджиталізації економічної діяльності. Управління ризиками в підприємствах

залежить від безпекових заходів та зовнішньо-політичного оточення, що пов'язано з існуючими можливими кібератаками на ресурси, інфраструктурні системи та технології, використанням не сумлінних інструментів конкурентної боротьби та цифровізації великих даних, ресурсів і інформації.

Управління ризиками в підприємствах залежить від чіткого виявлення впливу та взаємозв'язків різноманітних чинників на ці процеси, коли визначені кількісні параметри ризиків і коли менеджер, який ухвалює управлінські рішення, може контролювати поточний стан процесів і затверджувати відповідні заходи опираючись на об'єктивну інформацію. Оскільки ідеальних рішень щодо управління ризиками поки що не існує, усі ризикові явища та процеси повинні безперервно вивчатися для виявлення слабких місць і недоліків, для розробки прийомів та методів, спрямованих якщо не на повне усунення, то принаймні на зменшення кількості цих слабких місць та неефективності. Складність, невизначеність та нестабільність умов функціонування підприємств, хаотичність зміни чинників, що їх формують, призвели до загострення прояву кризових процесів та зумовили виникнення економічних деформацій в підприємствах.

Розуміння керівниками й менеджерами внутрішніх можливостей підприємств створює передумови для управління ризиками та розробки відповідних напрямів активізації й стратегічних орієнтирів, адекватних викликам зовнішнього середовища. Виходячи з цього, можливості підприємств протистояти негативному впливу чинників значною мірою визначаються рівнем їх внутрішньої стійкості до ризиків, тобто, спроможності підприємств протистояти різного роду ризикам, що дозволяє визначити їх потенційну здатність досягти запланованих результатів, забезпечити сталий поступ за несприятливого впливу будь-яких ризиків в умовах цифровізації й нечіткого середовища. З метою оцінки внутрішньої стійкості до ризиків підприємств доцільно визначити основні параметри та сформувати відповідну систему індикаторів оцінки. Для формування системи показників оцінки впливу ключових чинників на управління ризиками підприємств слід залучати різноманітних експертів − керівників та фахівців підприємств. Кожному залученому експерту пропонується заповнити анкету, в якій необхідно висловити власну думку щодо включення показників у систему, на основі яких можливе встановлення „слабких сигналів", які можуть вплинути на порушення стійкості до ризику підприємств (додаток).

Експертне опитування слід проводити за методом Делфі. Даний метод є одним із найпоширеніших методів анкетування. Згідно з методом Делфі, кожен експерт отримує спеціально розроблену анкету з питаннями, яку заповнює незалежно від інших. Відповіді експертів підсумовують та разом із узагальненими безособовими аргументами на користь тих чи інших оцінок повертають експертам для уточнення чи зміни, якщо вони знайдуть це необхідним, своїх первісних відповідей [107, 116]. Перевагою застосування методу Делфі є забезпечення незалежності думок фахівців, що надає можливість через кількісну форму, сформувати систему показників. Так. на

основі результатів анкетування встановлено, що основними параметрами оцінки ризикостійкості підприємств є такі напрями: фінанси, персонал, матеріально-технічна база, маркетинг, інновації, за кожним з яких визначено основні індикатори оцінки та сформовано групи чинників впливу (рис. 2.6).

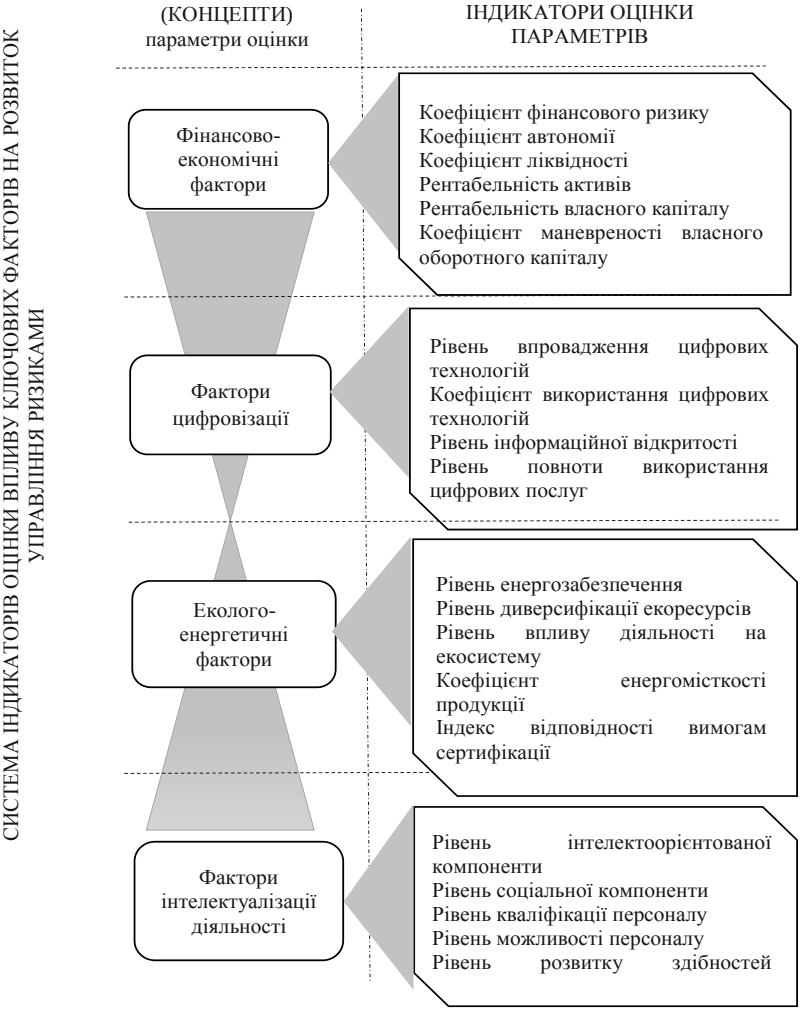


Рис. 2.6. Система індикаторів оцінки впливу ключових чинників на управління ризиками в підприємствах
Примітка: розроблено на основі [64, 172]

Водночас, експерти зазначили, що розроблена система індикаторів оцінки ключових чинників впливу на управління ризиками підприємств, повинна враховувати галузеву специфіку за концептами (фінансово-економічні чинники, чинники цифровізації, еколого-енергетичні чинники, чинники інтелектуалізації діяльності), що дозволить на основі встановленого рівня внутрішньої ризикостійкості до вказаних груп чинників визначити розвиток та можливості досягнення високих економічних результатів підприємствами.

З огляду на те, що використовується широкий спектр індикаторів, які мають бути враховані щодо рівня впливу чинників на управління ризиками підприємств, доцільно визначати інтегральний показник рівня внутрішньої стійкості до впливу чинників на розвиток управління ризиками (KFDR), який формується з урахуванням локальних інтегрованих оцінок за кожним параметром впливу чинників, відповідно: фінансово-економічні чинники, чинники цифровізації, еколого-енергетичні чинники, чинники інтелектуалізації діяльності. Такий підхід дозволить визначити стан окремих параметрів впливу, з метою ідентифікації „вузьких місць" у діяльності підприємств, що сприятиме деталізації процесу розробки комплексу заходів щодо мінімізації чи нівелювання ризиків за певними параметрам впливу чинників на управління ризиками. Для інтегрованої оцінки параметрів впливу чинників на управління ризиками варто використати наступний показник:

$$Кj = \sum_{k-1}^{n} \mathcal{L}_{k} \left[1 - \gamma_{of}\right]^{-1}$$

де: Кj − інтегрована оцінка j-го параметра впливу чинника на управління ризиками;

$\mathcal{L}_{k}$ – значимість k-го індикатора оцінки j-го параметра впливу чинника на управління ризиками;

γ_{of} − стандартизоване значення k-го індикатора оцінки j-го параметра впливу чинника на управління ризиками, який розраховується за формулою:

$$\gamma_{of} = (\gamma_i - \gamma_{min})/(\gamma_{max} - \gamma_{min}) \qquad (2.14)$$

де: γ_i – фактичне значення і-го індикатора оцінки j-го параметра фінансово-економічних чинників, чинників цифровізації, еколого-енергетичних чинників, чинників інтелектуалізації діяльності у k-му періоді, коеф.;

γ_{max}, γ_{min} – відповідно максимальне та мінімальне значення і-го індикатора оцінки j-го параметра фінансово-економічних чинників, чинників цифровізації, еколого-енергетичних чинників, чинників інтелектуалізації діяльності у k-му періоді, коеф.

Узагальнюючи вище проведені розрахунки, розглянемо блок-схему оцінок внутрішніх можливостей підвищення управління ризиками підприємств (рис. 2.7), що дозволяє чітко структурувати весь діагностичний процес, починаючи з визначення значення інтегрованих оцінок за концептами (фінансово-економічні чинники, чинники цифровізації, еколого-енергетичні чинники, чинники інтелектуалізації діяльності), а також оцінити фактичний

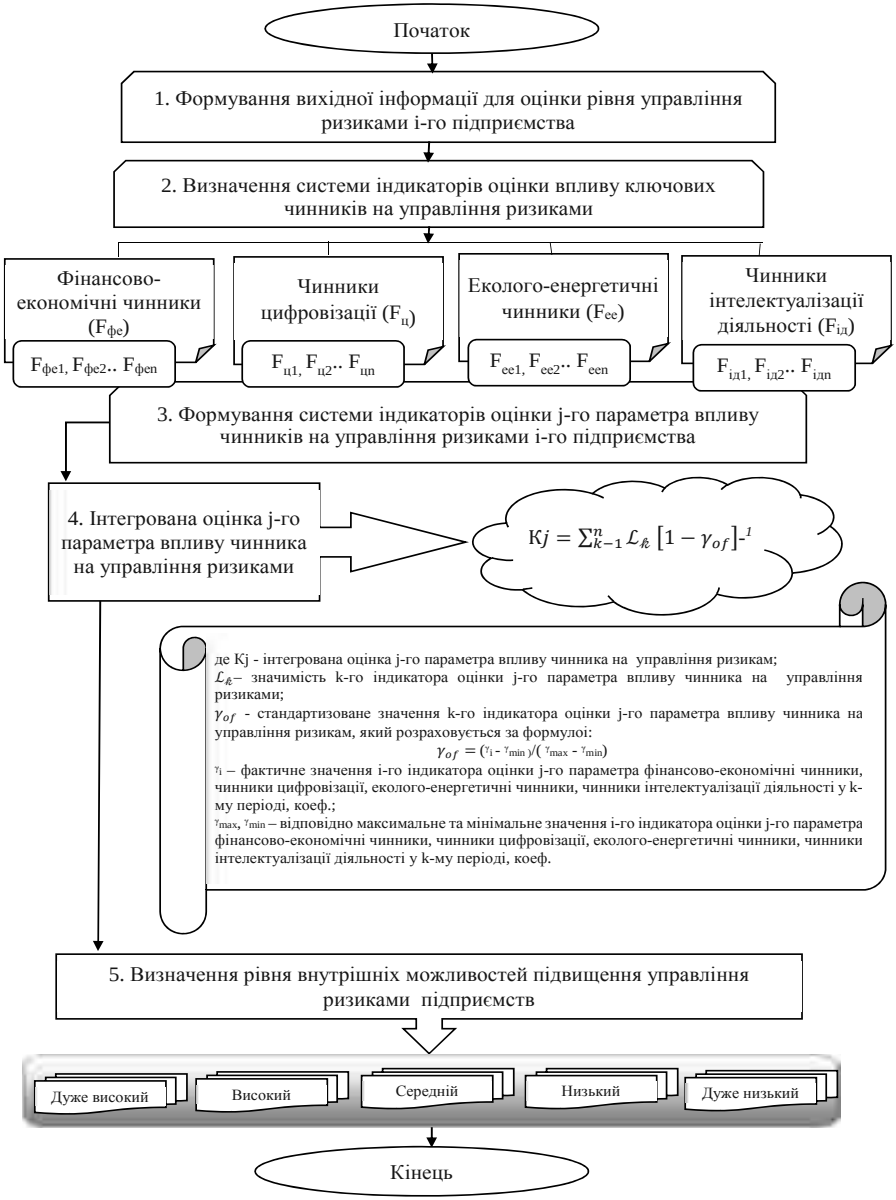


Рис. 2.7. Блок-схема визначення внутрішніх можливостей підвищення управління ризиками підприємств

Примітка: розроблено з використанням [105, 110, 111, 114]

рівень внутрішньої стійкості до ризиків, шляхом інтегрування до єдиної мети, завдань та об'єктів окремих етапів діагностики.

Таким чином, результати проведеної діагностики впливу чинників на управління ризиками засвідчать, чи активізацію такої діяльності можна вважати ключовим аспектом діяльності підприємств. З огляду на системний характер управління ризиками підприємств актуалізується питання оцінки внутрішніх можливостей щодо його активізації та гармонізації. Така діагностика дозволить правильно визначити вектор управлінських рішень щодо подальшого управління ризиками підприємств.

Так, розглядаючи характерні ризики окремих підприємств, доцільно акцентуватись на ризиках інформаційно-комунікаційних технологій, що пов'язані із надійністю та якістю білінгових систем, кібер-безпекою, захистом конфіденційної інформації, особливо персональних даних клієнтів підприємства. Означене, слід доповнити ризиками, зумовленими проведенням реструктуризації підприємств внаслідок поширених сьогодні процесів злиття та поглинання.

Водночас, нині, не можна оминути ризики, які стали вагомими для підприємств, воєнного та пост воєнного часу, зважаючи на те, що підприємства змушені функціонувати в жорстких умовах економічної кризи в наслідок жорсткої російської агресії. Втрати активів і ресурсів (кадрові, фінансові, матеріальні, територіальні (покриття), технологічні, інфраструктурні тощо) вимагають розробки нових підходів до формування системи управління ризиками в підприємствах задля забезпечення важливого компоненту життєстійкості й незламності населення та умов перемоги України – постійних комунікацій та надійного зв'язку.

Водночас, варто враховувати: реалізацію принципово нових технологічних рішень; невпинну інтеграцію до західноєвропейського інфо-комунікаційного ринку, формування єдиного цифрового простору з ЄС тощо. За означених нових економічних реалій життєво важливим є завчасне виявлення й об'єктивна діагностика ефективності управління ризиками в підприємствах та формування адаптивної системи управління ризиками із використанням проактивних методів їх мінімізації та нівелювання. Цікаво, що зарубіжні підприємства здійснюють безперервне управління ризиками на превентивній, антисипативній основі за слабкими сигналами загроз. Настання відчутних змін в динамічному середовищі вітчизняного підприємства теж відбувається не водночас, фактично перед такими змінам завжди проявляються сигнали раннього попередження, слабкі сигнали. Адекватна ідентифікація яких може завчасно попередити про загрози та ризики, що наближаються. Вплив ризикових процесів на функціонування підприємств спричиняє негативні наслідки їх фінансового стану: низька обіговість активів, незбалансованість грошових потоків, наявність значної частки дебіторської та кредиторської заборгованості у складі оборотних активів та поточних зобов'язань відповідно, висока собівартість послуг і продуктів, недостатня ліквідність та платоспроможність тощо.

Для виживання в сьогоднішніх економічних реаліях підприємствам необхідна наявність результативного своєчасного управління ризиками, що дасть змогу стежити за ринковими тенденціями, здійснювати глибоку експертизу діяльності конкурентів та оперативно реагувати на нові виклики та загрози сьогодення. До найбільш розповсюджених чинників, що пояснюють необхідність пошуку підприємствами нових підходів до діагностики ефективності управління ризиками на підприємствах в умовах цифровізації, та активізації цих процесів можна віднести: „генерування нових конкурентних переваг; прагнення збільшення капіталізації підприємства, зокрема з допомогою розміщення акцій на світових фондових біржах; розвиток нових послуг та тарифних схем; зростання абонентської бази операторів та ускладнення розрахунків" [149 с. 69]. Водночас, зауважимо, що окрім операційних бізнесових ризиків для підприємств знаковими вважаються й інвестиційні ризики, що зумовлено гостротою конкурентної боротьби, що змушує здійснювати вагомі додаткові інвестиції в інноваційні проекти щодо закупівлі сучасного обладнання та розвитку новітніх технологій. До таких новітніх технологій відносять: хмарні технології, широкосмуговий доступ до Інтернету, цифрове медіа та телебачення, послуги інтелектуальної мережі зв'язку, діджиталізацію бізнес-процесів з використанням елементів штучного інтелекту, організація відео конференцій, впровадження трафіку віртуальних мереж тощо. Наголосимо, що ключовим рішенням щодо подолання наслідків настання кризових явищ та прояву ризиків стало масове скорочення інвестиційних програм підприємствами. Аналіз статистичних даних провідних міжнародних організацій, які займаються систематизацією аналітичних показників розвитку галузі технологій та зв'язку різних країн світу та визначенням найбільш актуальних ризиків її функціонування, свідчить про існування певних проблем та тенденцій даної галузі. Відповідно даних Technology and Communications Industry Report [195], топовими ризиками підприємств в умовах цифровізації є зростання конкуренції, втрата репутації бренду підприємства, невідповідність інноваційним потребам клієнтів, втрата професійних кадрових ресурсів, кіберзлочини, часова нерівномірність економічних циклів, втрата інтелектуальної власності, нестабільність нормативно-правової бази, недосконаліть інформаційних технологій та порушення ланцюгів постачань продуктів. Зазначені ризики було структуровано за ступенем їх впливу (від 1 до 10 місця) (табл. 2.3).

Джерелом наведеної інформації є результати опитування респондентів різних країн, яким було запропоновано обрати 10 найбільш вагомих ризиків для їх власних підприємств із 53 ризиків загального переліку [105].

Найбільш актуальними було виявлено ризики зростання конкуренції, втрати репутації бренду та невідповідності інноваційним потребам клієнтів.

Слід зазначити, що конкуренція як невід'ємний атрибут ринкових відносин активізує розвиток інноваційного потенціалу підприємств, стимулює продуктивність їх діяльності та економічне зростання.

Таблиця 2.3

Ризики підприємств в умовах цифровізації

Місце	Сфера технологій та зв'язку *(Technology and Communications Industry)*	Сфера технологій *(Technology)*	Сфера комунікацій *(Communications)*
1	Технологічні ризики (недосконаліть ІКТ)	Виробничі ризики (порушення ланцюгів постачань продуктів, ризик часової нерівномірності економічних циклів)	Підприємницькі ризики (зростання конкуренції, втрата репутації бренду)
2	Ризики діджиталізації	Кібер- ризики (кіберзлочинність)	Ризик втрати професійних кадрових ресурсів та інтелектуальної власності
3	Виробничі ризики (порушення ланцюгів постачань продуктів, ризик часової нерівномірності економічних циклів)	Технологічні ризики (недосконаліть ІКТ)	Ризики діджиталізації
4	Підприємницькі ризики (зростання конкуренції, втрата репутації бренду)	Підприємницькі ризики (зростання конкуренції, втрата репутації бренду)	Виробничі ризики (порушення ланцюгів постачань продуктів, ризик часової нерівномірності економічних циклів)
5	Кібер- ризики (кіберзлочинність)	Інвестиційні ризики	Технологічні ризики (недосконаліть ІКТ)
6	Інвестиційні ризики	Адміністративно-нормативні ризики (ризик злиття та поглинання підприємств, ризик банкрутства)	Інноваційні ризики (невідповідність інноваційним потребам клієнтів)
7	Ризик втрати професійних кадрових ресурсів та інтелектуальної власності	Юридичні ризики (нестабільність нормативно-правової бази, ризик корпоративної відповідальності)	Кібер- ризики (кіберзлочинність)
8	Інноваційні ризики (невідповідність інноваційним потребам клієнтів)	Ризик втрати професійних кадрових ресурсів та інтелектуальної власності	Інвестиційні ризики

9	Адміністративно-нормативні ризики (ризик злиття та поглинання підприємств, ризик банкрутства)	Інноваційні ризики (невідповідність інноваційним потребам клієнтів)	Юридичні ризики (нестабільність нормативно-правової бази, ризик корпоративної відповідальності)
10	Юридичні ризики (нестабільність нормативно-правової бази, ризик корпоративної відповідальності)	Ризики діджиталізації	Адміністративно-нормативні ризики (ризик злиття та поглинання підприємств, ризик банкрутства)

Примітка: сформовано з використанням [105].

Поруч з цим, ризик зростаючої конкуренції може привести до припинення діяльності недостатньо капіталізованих та фінансово нестійких підприємств, що пояснюється наявністю конкурентів з боку іноземних компаній, стрімким розвитком технологій, зміною тарифної політики тощо. З огляду на це більшість підприємств розглядають конкуренцію як пріоритетний ризик сучасності, який в цілому займає перше місце. Слід зазначити, що ризик невідповідності інноваційним потребам клієнтів є доволі актуальним для вітчизняних підприємств, які демонструють недостатній рівень інноваційної активності. Це зумовлено існуванням низки чинників, серед яких можна виділити фінансові (нестача власних фінансових ресурсів, значні витрати на освоєння інновацій, тривалість окупності нових цифрових продуктів, брак коштів у замовників) – 39%; інформаційні (дефіцит інформації щодо нового обладнання чи цифрових технологій, відсутність даних щодо існуючих тенденцій розвитку ринків, проблеми зі знаходженням зацікавлених учасників щодо партнерства у сфері інноватики) – 19%; ринкові (домінування окремих підприємств на ринку окремих послуг, низький попит на інноваційні продукти чи цифрові технології, високі економічні та фінансові ризики при освоєнні цифрових нововведень на підприємстві) – 27%; інші (немає необхідності у швидкому впровадженні інновацій, недосконалість нормативного поля у сфері підтримки підприємств, нестача або відсутність досвідчених кваліфікованих спеціалістів для освоєння інновацій) – 15% [105].

2.2. Ризикозахищеність підприємства в умовах цифровізації

Процеси цифровізації підприємств зазнають істотного впливу елементів невизначеності, чим зумовлюється високий ризик їх діяльності. Цей ризик стає особливо значним, оскільки багато важливих рішень приймаються в умовах неповної, неточної чи суперечливої інформації.

Наслідком прийняття рішень в умовах цифровізації є невизначеність результатів, тому доводиться ризикувати. З іншого боку, ризик викликаний спонтанним і суперечливим характером цифрових процесів, що відбуваються в

складних соціально-економічних системах, які неможливо адекватно і вичерпно описати.

Таким чином, ризик підприємств в умовах цифровізації, слід розглядати як наслідок прийняття рішень в умовах неповної, неточної чи суперечливої інформації, тобто в умовах невизначеності чи неповної визначеності.

Під ризиком цифровізації розуміють можливість (загрозу) втрати підприємством частини своїх ресурсів, недоотримання доходів чи виникнення додаткових витрат у результаті здійснення виробничо-збутової і фінансової діяльності, яка спирається на нові цифрові технології, нові продукти, нові способи їхньої реалізації тощо. Численні техногенні катастрофи, кількість яких зростає в міру розвитку цифрових технологій, підтверджують це.

При здійсненні цифрових трансформацій у підприємств виникає об'єктивна необхідність у розробці способів попередження, зниження чи компенсації можливих негативних наслідків цих специфічних ризиків. Для цього підприємства спочатку кількісно оцінюють величину ризику конкретного процесу цифровізації (як ймовірності деструктивних наслідків, так і величини можливих втрат), виділяють і досліджують вплив і частку кожного з чинників ризику в загальному обсязі можливих втрат. Результати оцінки ризику враховують при ухваленні підприємствами рішень щодо вибору стратегії і тактики цифрового розвитку, плануванні науково-технічної, виробничо-збутової і фінансової діяльності, що пов'язана із цими процесами.

Ризик може проявлятися в тому, що новий (модернізований) продукт чи послуга вже в процесі впровадження виявляється непотрібним, тоді як на момент рішення про його розробку і впровадження, що спиралося на результати діагностикиа кон'юнктури ринку, потреб і запитів споживачів, напрямків і темпів розвитку НТП тощо, передбачалося, що попит на нього буде стійким.

Ризик може проявлятися й у тому, що на даному ринку чи його сегменті новий продукт чи послуга можуть бути і не реалізованими у тих обсягах, які були розраховані на основі результатів маркетингових досліджень. Ухвалюючи рішення про проведення великомасштабної рекламної компанії нової продукції, зазвичай, не можна бути цілком упевненим у її ефективності. Так само, як і вибираючи варіанти цінової стратегії для проникнення на нові ринки, не можна з повною впевненістю стверджувати, що підприємство очікує успіх, оскільки конкуренти можуть відповісти адекватними діями.

Як наслідок цих ситуацій – можливість отримання збитків чи недоотримання доходу. Тому, впровадження цифрових трансформацій підприємствами завжди пов'язано з високим ризиком.

Основні причини цього:

можливі різкі зміни економічної, політичної, соціальної, екологічної і інших складових середовища функціонуванняа в процесі впровадження цифрових трансформацій;

зміни споживчих запитів;

несприйнятливість інноваційних цифрових трансформацій персоналом чи споживачами;

непередбачуваність дій конкурентів;

неадекватна оцінка власних можливостей;

прискорення темпів науково-технічного прогресу, цифрові технологічні і технічні прориви тощо.

У цих реаліях, підприємствам необхідно особливо ретельно прогнозувати і кількісно оцінювати ризик цифровізації з урахуванням усього комплексу чинників ризику з метою розроблення пулу заходів, спрямованих на зниження, компенсацію чи запобігання можливим деструктивним наслідкам. Причому цю оцінку підприємствам доводиться вести в умовах інформаційного дефіциту, що вимагає специфічних методів оцінки ризику.

Оцінка ризику підприємств в умовах цифровізації поділяється на два доповнюючих один одного види – якісна і кількісна.

Якісна оцінка має за мету визначення чинників ризику, що впливають на результати прийнятих рішень і виконуваних робіт, встановлення потенційних зон ризику й ідентифікацію ризиків.

Кількісна оцінка передбачає чисельне визначення розмірів ризику (ймовірностей виникнення втрат і їх величин).

При оцінці ризику часто виділяють ті їх види, що не пересікаються, для того щоб уникнути подвійного урахування.

Часто для кількісної оцінки ризику використовують імовірнісний підхід, відповідно до якого для того, щоб оцінити ризик, необхідно знати всі можливі наслідки конкретного рішення чи дії (або закон їхнього розподілу) і ймовірності цих наслідків.

Імовірності розвитку того чи іншого сценарію визначають:

об'єктивним методом (на підставі наявних даних про аналогічні проекти, що виконувалися в аналогічних умовах, розраховується частота, з якою відбуваються ті чи інші явища);

суб'єктивним методом (зокрема, шляхом експертної оцінки, коли група експертів висловлює припущення щодо конкретних результатів і ймовірностей їхнього виникнення).

Імовірнісний підхід для оцінки ризику передбачає використання таких критеріїв:

очікуване значення результату, яке розраховується як середньозважене за ймовірностями величин усіх можливих результатів (як результат звичайно використовують запланований прибуток (доход) конкретного процесу цифровізації або можливі втрати);

мінливість чи розкид можливих результатів, що розраховується як корінь квадратний із середньозваженого квадратів відхилень можливих результатів від їх очікуваного значення (середньоквадратичне чи стандартне відхилення).

Іноді виникають ситуації, коли корисним виявляється розрахунок такого критерію, як відносний ризик (величина ризику, що припадає на одиницю результату), щоб перевірити, чи компенсується підвищений ризик підвищеним доходом. Показник даного критерію розраховується як результат від ділення

середньоквадратичного відхилення на очікуване значення результату (у статистиці йому відповідає коефіцієнт варіації).

Слід відзначити, що використання критерію відносного ризику можливе лише у випадку, якщо очікувані значення результатів за варіантами порівнянні. В іншому випадку даний критерій не застосовується.

Для оцінки ризику цифровізації, підприємства використовують різні методи, серед яких найбільше поширення одержали статистичний метод (у тому числі метод статистичних випробувань чи метод Монте-Карло); аналітичний метод; метод використання дерева рішень та імовірнісного підходу; метод оцінки фінансової стійкості або оцінки доцільності витрат; метод експертних оцінок; нормативний метод; метод діагностикиа чутливості; метод використання аналогів та інші.

Кожний з названих методів має свої переваги і недоліки і використовується в цілком конкретних ситуаціях; універсального методу, прийнятного для всіх випадків, не існує. В практичній діяльності, підприємства використовують декілька методів. Природно, отримані різними методами результати різняться, але дослідження розходжень між ними дозволяють виявити чинники, які враховуються в одних методах і відсутні в інших, що впливає на точність оцінки і достовірність результатів.

Аналіз розходжень у результатах дасть змогу виявити існуючі тенденції розвитку майбутніх подій з погляду ризику тих чи інших процесів цифровізації. А це сприятиме більш точному прогнозуванню ступеня ризику конкретних проектів цифрових трансформацій.

У деяких випадках підприємства використовують інші, більш специфічні методи, що включають у різних комбінаціях елементи теорії ігор, теорії оптимізації, чинникного аналізу, теорії ймовірностей (у тому числі умовні ймовірності), комбінаторики, нечіткої логіки тощо.

Цікаво, що понад 90% підприємств, що впроваджували цифрові трансформації, істотно поліпшили показники своєї діяльності і зміцнили свої позиції на ринку.

Водночас, цифрові трансформації, в результаті яких підвищуються невизначеність, ризик і загрози, особливо гостро випинають проблематику виявлення можливостей ризикозахищеності підприємств, оскільки вони функціонують в кризових умовах конкурентного середовища, володіючи різної потужності цифровим потенціалом. Тому у кожного підприємства генеруються специфічні ризики та загрози, що притаманні лише конкретному підприємству.

Т. Андерсен та П. Шредер стверджують, що „нині, коли відбуваються корпоративні скандали і великі фінансові невдачі, підвищується актуальність ефективного управління ризиками”.

І. Кох обґрунтовує „застосування нечітких моделей для оцінки ризиків”. Підтримують такий підхід і Мамдані, Сугено, Цукамото.

А. Гріффін, наводить конкретні приклади „ефективних і помилкових дій корпорацій з управління ризиками”.

Т. Бедфорд і Р. Кук окреслюють „фундаментальні поняття невизначеності, її співвідношення з ймовірністю, межі з кількісною оцінкою невизначеності".

„Ризикозахищеність підприємства − це забезпеченість життєво важливих інтересів і потреб системи підприємства від усього спектра зовнішніх і внутрішніх загроз, різних за своєю природою". У контексті системного підходу, ризикозахищеність підприємства в умовах цифровізації окреслюється, як „властивість системи, що забезпечує її сталий і стабільний цифровий розвиток в умовах виникнення різних видів ризиків внутрішнього і зовнішнього середовища.

Тобто, це така характеристика системи, яка дозволяє звести до мінімуму, а в кращому випадку, і повністю позбутися від негативних наслідків впливу ризиків різної природи". Практично, ризикозахищеність підприємства в умовах цифровізації демонструє спроможність підприємства успішно протидіяти ендогенним і екзогенним загрозам, можливість адекватно і швидко трансформувати свій організаційний дизайн й цифровий потенціал відповідно до динамічних реалій.

У розвиток такого підходу, управління ризикозахищенністю підприємства в умовах цифровізації окреслюють, як багатоступінчастий комплексний процес, метою якого вважається зниження чи компенсація втрат на підприємстві за реалізації ризиків при освоєнні цифрових інновацій.

Наукові підходи до обґрунтування сутності, витоків генерування і різновидів ризиків цифрових трансформацій досить строкаті. Мета знаходження можливостей ризикозахищеності підприємства в умовах цифровізації має дисонувати цільовій функції підприємства щодо генерування максимальних обсягів прибутку при гармонійному співвідношенні прибутку і ризику.

Концептуальні підходи щодо можливості ризикозахищеності підприємства в умовах цифровізації зосереджені у такому:

цифрові трансформації підприємства завжди супроводжуються ризиком як атрибутом невизначеності;

на виникнення ризику та його значимість впливають чинники зовнішнього та внутрішнього середовища, тож доцільно вивчати зовнішні та внутрішні чинники виникнення ризиків цифрової трансформації;

ризик може мати як деструктивний характер, тобто приносити збитки підприємству, так і позитивний, тобто підсилювати приховані можливості цифрового розвитку;

незалежно від характеру прояву ризику необхідно ним управляти, використовуючи такі методи як, страхування, лімітування, диверсифікація, хеджування тощо.

Тож, зважаючи на означене щодо можливості ризикозахищеності, на рисунку 2.8 представлено конститутивні атрибути ризикозахищеності підприємства в умовах цифровізації.

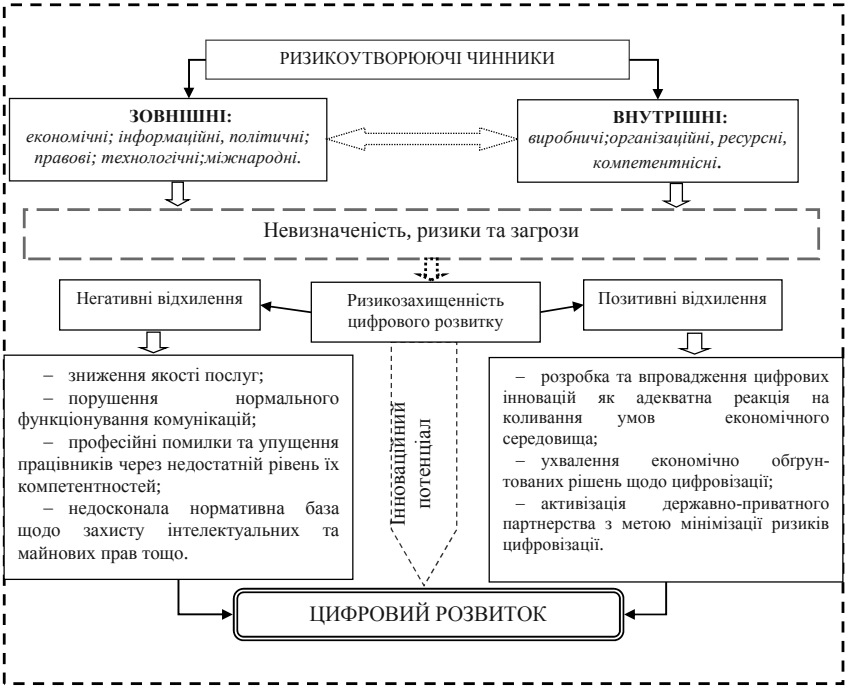


Рис. 2.8. Конститутивні атрибути ризикозахищеності підприємства в умовах цифровізації

Види ризиків підприємства в умовах цифровізації представлено на рисунку 2.9.

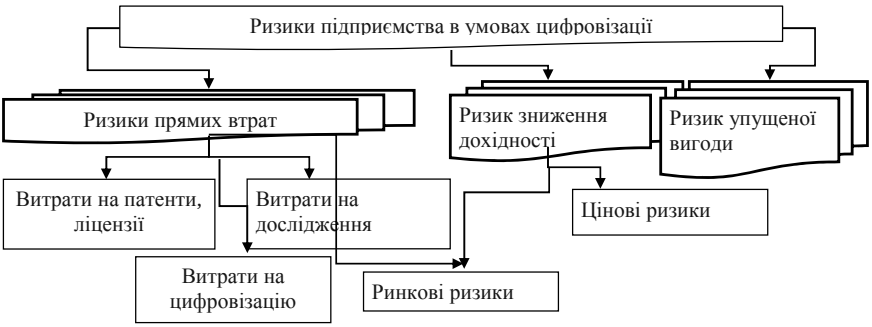


Рис. 2.9. Ризики підприємства в умовах цифровізації

Система внутрішніх та зовнішніх чинників, що впливають на виникнення ризиків в підприємствах в умовах цифровізації продемонстрована на рисунку 2.10.

Рис. 2.10. Система внутрішніх та зовнішніх чинників, що впливають на виникнення ризиків в підприємствах в умовах цифровізації

За результатами експертних оцінок щодо ризиків внутрішнього середовища, з'ясовано (табл. 2.4), що гальмуючими чинниками цифрових трансформацій підприємств є: відсутність фінансових джерел для впровадження цифрових трансформацій (16 %), низька активність освоєння цифрових трансформацій (15 %), низькі ринкові можливостей й альтернативи втілення цифрових трансформацій (14 %), відсутність стратегічного набору (12 %), низька організаційно-комунікаційна здатність щодо цифрових трансформацій (11 %), нерозвинутість організаційного дизайну та комунікаційних внутрішніх зв'язків (9 %), незацікавленість управлінської команди (7 %), відсутність спеціалістів з відповідними компетенціями (6 %), нерозвиненість інфраструктури цифрових трансформацій (5 %), низький рівень диверсифікації діяльності (3 %), високий рівень формалізації й централізації менеджменту (2 %).

Таблиця 2.4

Ризики внутрішнього середовища, що гальмують цифрові трансформації підприємств

Ризик	Вага ризиків
Відсутність фінансових джерел для впровадження цифрових трансформацій	0,16
Низька активність освоєння цифрових трансформацій	0,15
Низькі ринкові можливостей й альтернативи втілення цифрових трансформацій	0,14
Відсутність стратегічного набору	0,12
Низька організаційно-комунікаційна здатність щодо цифрових трансформацій	0,11
Нерозвинутість організаційного дизайну та комунікаційних внутрішніх зв'язків	0,09
Незацікавленість управлінської команди	0,07
Відсутність спеціалістів з відповідними компетенціями	0,06
Нерозвиненість інфраструктури цифрових трансформацій	0,05
Низький рівень диверсифікації діяльності	0,03
Високий рівень формалізації й централізації менеджменту	0,02

Таблиця 2.5

Ризики зовнішнього середовища, що гальмують цифрові трансформації підприємств

Ризики	Вага ризиків
Високі параметри кредитних ставок	0,19
Обтяжлива система оподаткування	0,17
Брак необхідної інфраструктури для трансферу цифрових технологій та відповідної інформаційно-аналітичної підтримки	0,15
Високий рівень конкурентної боротьби	0,12
Відсутність необхідності впровадження цифрових трансформацій	0,10
Зростання інфляційних процесів, що впливає на високу вартість матеріальних активів, технологій, енергоносіїв	0,09
Відсутність налагоджених зв'язків між наукою та виробництвом	0,08
Низька платоспроможність населення	0,05
Нерозвиненість мережі цифрової інфраструктури	0,03
Недостатнє державне стимулювання цифрових трансформацій	0,02
Неочікувані зміни керівництва та завдань цифрового розвитку, рейдерство	0,01

За результатами експертних оцінок щодо ризиків зовнішнього середовища (табл. 2.5), з'ясовано, що гальмуючими чинниками цифрових трансформацій підприємств є: високі параметри кредитних ставок (19 %), обтяжлива система оподаткування (17 %), брак необхідної інфраструктури для трансферу цифрових технологій та відповідної інформаційно-аналітичної підтримки (15 %), високий рівень конкурентної боротьби (12 %), відсутність

необхідності впровадження цифрових трансформацій (10 %), зростання інфляційних процесів, що впливає на високу вартість матеріальних активів, технологій, енергоносіїв (9 %), відсутність налагоджених зв'язків між наукою та виробництвом (8 %), низька платоспроможність населення (5 %), нерозвиненість мережі цифрової інфраструктури (3 %), недостатнє державне стимулювання цифрових трансформацій (2 %), неочікувані зміни керівництва та завдань цифрового розвитку, рейдерство (1 %).

Зважаючи, що ризик впливає на можливість здійснення руйнівних наслідків цифрового розвитку, і водночас може сприяти генеруванню додаткових можливостей, усі методи доцільно сегментувати на: методи зменшення рівня чинників ризику цифрових трансформацій; методи підсилення сприятливих можливостей ризикозахищеності (рис. 2.11).

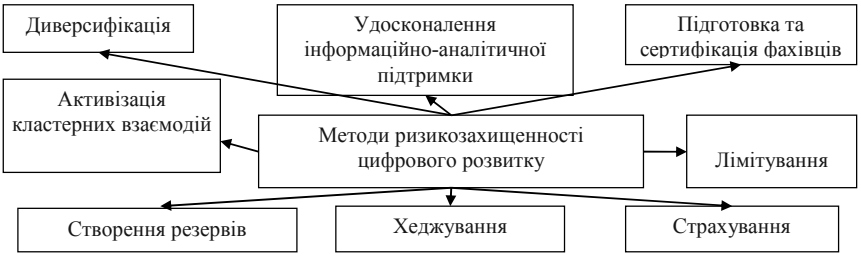


Рис. 2.11. Методи ризикозахищеності підприємств в умовах цифровізації

Дієвий стратегічний набор управління ризикозахищеністю підприємствах в умовах цифровізації має бути зорієнтований на гармонізацію співвідношення бажаного прибутку і величини ризику. Важливим інструментом для зменшення невизначеності та оптимізації такого співвідношення вважаємо розвиток інформаційно-аналітичної підтримки цифрового розвитку підприємств.

Розробка карти ризиків цифрових трансформацій підприємства та його ризик-профілю буде доцільною при: оцінці загроз і ризиків; формуванні стратегічного набору за показниками ризикозахищеності; прогнозуванні заходів на підтримку функціонування системи ризикозахищеності підприємства та необхідних витрат.

Прийняття управлінських заходів щодо забезпечення ризикозахищеності підприємствах в умовах цифровізації має опиратись на ключові принципи: не доцільно ризикувати на суму більшу власних активів; завжди потрібно розраховувати вплив наслідків ризику; не слід ризикувати великою сумою заради малих прибутків; позитивно ухвалюється рішення тільки при відсутності альтернатив, якщо є альтернативи, то слід ухвалювати превентивні дії щодо мінімізації ризиків (рис. 2.12).

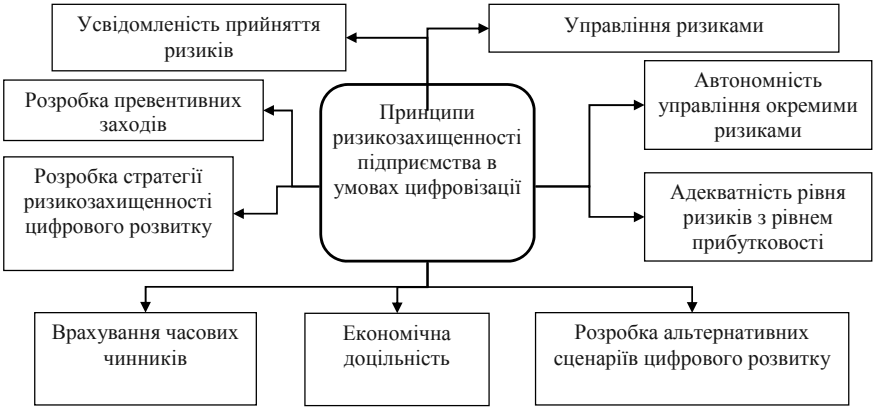


Рис. 2.12. Принципи ризикозахищеності підприємств в умовах цифровізації

Вказані принципи є загальними, тобто вони є сукупністю правил розробки заходів, яких доцільно притримуватись при різних сценаріях розвитку подій. Обов'язково, при формуванні і фільтрації стратегічного набору необхідно враховувати часові і ресурсні обмеження. На рисунку 2.13 подано механізм ризикозахищеності підприємства в умовах цифровізації.

Відповідно до обґрунтованих положень система заходів щодо ризикозахищеності підприємств в умовах цифровізації має включати:

постійний моніторинг і аналіз ризиків та ендогенних й екзогенних чинників й передумов здійснення цифрового розвитку підприємств;

розробка системи заходів щодо мінімізації зовнішньої уразливості цифрового розвитку підприємств;

підвищення гнучкості організаційного дизайну та формування структур, що займаються ризикозахищеністю підприємств в умовах цифровізації;

розробка превентивних заходів щодо мінімізації наслідків реалізації ризиків та появи перешкод для цифрового розвитку підприємств;

підготовка персоналу та розробка відповідних заходів щодо розподілу відповідальності і повноважень при настанні непередбачуваних чи кризових ситуацій.

Цифровий розвиток відбувається нерівномірно, демонструє висхідні та низхідні періоди, коливання кількісних та якісних економічних характеристик, конструктивні та руйнівні тренди і має розглядатися в певному часовому відтинку. Такий підхід до формування можливостей ризикозахищеності підприємств в умовах цифровізації сприятиме їх цифровому розвитку, підвищенню їх конкурентоспроможності та нарощуванню ефективності.

Рис. 2.13. Механізм ризикозахищеності підприємств в умовах цифровізації

2.3. Управління ризиками цифровізації підприємств

За останній часовий період досить гостро вип'ятилась проблема загрози ризиків цифровізації, що пояснюється процесами глобалізації, інтеграції та диджиталізації, що відмітили 38% респондентів, також вагомий вплив несуть на діяльність підприємств інвестиційні ризики – 25% респондентів підтвердили цей тренд загроз. Так, „вразливість інформаційних інфраструктур сягає – 40% за похибками у налаштуванні, 27% становлять помилки у програмному коді та

20% ризики відсутності або несвоєчасність оновлень безпекових програм" [87]. Мінімальний безпосередній вплив на діяльність підприємств здійснюють адміністративно-нормативні та юридичні ризики.

Кожен технологічний бізнес-процес підприємства в умовах цифровізації піддається загрозам безпеки і конфіденційності. Сучасні засоби захисту здатні боротися з атаками кіберзлочинців. Але цього недостатньо – тому підприємство повинно забезпечити такі умови внутрішньої політики і поведінки співробітників, щоби мінімізувати або значно зменшити ризики цифровізації.

Поняття безпеки цифровізації підприємства включає:

надійність роботи мережі комп'ютерів;

збереження цілісності інформаційного масиву (неправомірна зміна даних);

захист інформаційного масиву від несанкціонованого доступу (здійснення дій, що унеможливлюють чи утруднюють доступ до ресурсів інформаційної системи);

таємниця електронного листування, забезпечення конфіденційності.

До внутрішніх загроз цифровізації відносять:

виток інформації;

неавторизований доступ.

До зовнішніх загроз цифровізації відносять:

шкідливі програми (віруси, трояни, черв'яки тощо;

атаки хакерів;

Ddos-атаки;

таргінг атаки;

спам;

фішинг;

промислові загрози (stuxnet, flame, duqu);

шпигунське програмне забезпечення (spyware, adware);

botnets (ботнети або зомбі-мережі).

Основні вразливості підприємств в умовах цифровізації виникають внаслідок дії наступних чинників:

недосконаліть програмного забезпечення, апаратної платформи;

різні характеристики будови автоматизованих систем в інформаційному потоці;

частина процесів функціонування систем є неповноцінною;

неточність протоколів обміну інформацією та інтерфейсу;

складні умови експлуатації і розташування інформації.

Система ризикозахищенності підприємства в умовах цифровізації має ґрунтуватися на трьох фундаментальних принципах управління:

принцип розімкнутого керування;

принцип компенсації;

принцип зворотного зв'язку.

За принципом розімкнутого управління створюються власні політики ризикозахищенності, виконання яких контролюється відповідальними

особами. Нині, у більшості великих підприємств виділяють спеціалістів, відповідальних за розробку і реалізацію політик ризикозахищенності, позицію CISO (Chief Information Security Officer) – керівника відділу IT-безпеки або директора по IT-безпеці.

Принцип компенсації має на увазі, що в разі виникнення будь-яких відхилень від розробленої політики ризикозахищенності або зовнішніх чинників (а це неминуче, оскільки підприємства розвиваються, з'являються нові загрози, приходять і йдуть нові співробітники, з'являються нові програмні продукти) необхідно негайно вносити відповідні корективи в алгоритм управління, що компенсували б негативний результат зовнішніх впливів.

Тому для підприємства в умовах цифровізації дуже важливо не тільки розглядати інциденти, що вже відбулися, але і будувати систему проактивного захисту, здатної відбити атаки до того, як з'являться проблеми, і навіть до того, як стане відомо про потенційні проблеми та слабкі місця.

Дуже важливо дотримуватися принципу зворотного зв'язку, що дозволяє управляти ризикозахищенністю за замкнутим колом. За цим принципом будуються багато систем цифрової безпеки.

Наявність ланки зворотного зв'язку в системі управління цифровою безпекою дозволяє не тільки виявити окрему загрозу, але і відреагувати на низку подій, на перший погляд ніяк не пов'язаних між собою. У цьому можуть допомогти цифрові продукти, що забезпечують централізоване зіставлення інформаційних даних журналів подій з мережевих пристроїв і систем безпеки в режимі реального часу, автоматично зіставляючи дані і виділяючи події і загрози ризикозахищенності підприємства в умовах цифровізації, що вимагають прийняття рішучих заходів, такі як Check Point Eventia Analyzer.

Побудова систем ризикозахищенності підприємства в умовах цифровізації з урахуванням вказаних принципів дає змогу використовувати існуючі методи оптимізації для покращення різних показників якості системи, таких як стійкість і гнучкість управління, швидкість реакції на існуючі та латентні загрози.

Велику шкоду підприємствам в умовах цифровізації завдають хакерські атаки.

Хакери – це електронні „взламники", які проникають в комп'ютерну систему, використовуючи особливі уразливі лазівки у програмному забезпеченні. Захиститися від них можна за допомогою особливого додатку – мережевого екрану з пакетною фільтрацією, що входить до складу антивірусних програм і робить комп'ютер невидимим для хакерів.

Для захисту від шкідливого коду і хакерських атак:

встановлюється антивірусна програма;

встановлюється оновлення ОС Windows (Update), що відповідає за безпеку;

увага при роботі зі спамом в електронній пошті і системах миттєвих повідомлень;

збереження резервної копії (BackUp) даних.

Технологія інфраструктури відкритих ключів дозволяє перевіряти і засвідчувати справжність користувача. Інфраструктура відкритих ключів або PKI забезпечує єдину ідентифікацію, аутентифікацію і авторизацію користувачів системи, додатків і процесів і разом з цим гарантує доступність, цілісність і конфіденційність інформації.

Інфраструктура PKI являє собою систему цифрових сертифікатів, носіями яких є USB-ключі або смарт-карти.

При використанні індивідуального секретного пароля і засобів криптографічного захисту, цифрові сертифікати отримують роль електронних паспортів.

Доцільно для ризикозахищенності підприємства в умовах цифровізації використовувати системи багаточинникної аутентифікації, що засновані на технології одноразових паролів (one time password) OTP призначені для аутентифікації мобільних користувачів, які відрізняється простотою у використанні, установці і адмініструванні.

Дана технологія заснована на тому, що пароль користувача не постійний і змінюється з плином часу спеціальним пристроєм (апаратним або програмним) – токеном. Дане рішення широко використовується в системах віддаленого доступу, в тому числі системах клієнт-банк, для аутентифікації користувачів при доступі з небезпечних середовищ (Інтернет-кафе, бізнес-центри тощо).

Також варто для захисту підприємства в умовах цифровізації використовувати біометричні системи. Біометричні системи – це вимірні фізіологічні або поведінкові дані людини (візерунки сітчатки ока; відбитки пальців; геометрія руки; динаміка підпису).

Біометричні дані унікальні для кожної людини і їх можна використовувати для встановлення особи або перевірки декларованих особистих даних:

для ідентифікації користувача (замість введення імені користувача);

для одночинникної аутентифікації користувача;

спільно з паролем або аутентифікаційї токеном (таким, як смарт- карта) для забезпечення двочинникної аутентифікації.

Доцільно для ризикозахищенності підприємства в умовах цифровізації використовувати й криптографію. Криптографія – область знань, що вивчає тайнопис (криптографія) і методи його розкриття (криптоаналіз). Криптографія вважається розділом математики.

Мета криптографічної системи полягає в тому, щоби зашифрувати вихідний текст (шифротекст, криптограма).

Основні тенденції застосування шифрування:

шифрування окремих файлів;

шифрування окремих розділів на жорсткому диску, віртуальних дисків;

шифрування жорстких дисків цілком.

Для ризикозахищенності підприємства в умовах цифровізації широко використовують електронний підпис. Електронний підпис – послідовність

символів, отримана в результаті криптографічного перетворення вихідної інформації з використанням закритого ключа ЕЦП, яка дозволяє підтверджувати цілісність і незмінність цієї інформації, а також її авторство за умови використання відкритого ключа ЕП і його сертифіката.

Сьогодні більшість підприємств використовують багаторівневі системи обробки інформації – комп'ютери, хмарні сховища, корпоративні мережі тощо.

Але ж, усі ці системи не тільки передають дані, але вони є і середовищем їх можливого витоку. Витік секретної інформації – процес неконтрольованого розголошення ключових даних.

Кожен співробітник підприємства є потенційною загрозою для ризикозахищенності. Часто співробітники забирають роботу додому – переміщують робочі файли на свої флеш-носії, передають їх по незахищеним каналам з'єднання, обговорюють інформацію зі співробітниками конкуруючих підприємств.

Ризик витоку інформації від персоналу є завжди, і його не можна виключити повністю.

На практиці виявити людину, що зливає комерційну таємницю, можна за такими ознаками:

співробітник без попередження затримується після роботи на своєму робочому місці;

співробітник зберігає на свій персональний комп'ютер або смартфон занадто багато електронних документів підприємства;

співробітник без необхідності копіює паперовий документообіг електронним (сканує документи або фотографує їх);

співробітник регулярно порушує загальні вимоги безпеки при роботі з комерційною таємницею;

співробітник був викритий в контактах із службовцями конкуруючих підприємств.

Для захисту технічних каналів витоку інформації, доцільно використовувати:

тепловізор (за допомогою такого девайса можна просканувати всі стіни і частини інтер'єру на наявність закладних пристроїв – жучків, відеокамер);

пристрої, що заглушають подачу сигналу радіочастот;

засоби захисту архітектурних конструкцій – ущільнювачі для вікон, дверей, підлоги і стелі (вони ізолюють звук і унеможливлюють зчитування вібраційних хвиль з поверхні будівлі);

пристрої для екранування і зашумлення (вони використовуються для захисту електромагнітного каналу витоку).

Також слід заземлити всі комунікації, що виходять за межі приміщення і контрольованої зони (труби, кабелі, лінії зв'язку).

Захищати треба не тільки електронні документи, а й всю друковану документацію, що містить секретні відомості. Відповідно до Закону України „Про зберігання і обробку відомостей, що містять комерційну таємницю", слід виконувати такі вимоги:

зберігати всі документи з комерційною таємницею виключно в окремих закритих приміщеннях, що охороняються цілодобово системами відеоспостереження або охоронцями;

доступ до службової (комерційної) таємниці можуть мати тільки співробітники, яким вона потрібна в процесі роботи;

запис про вилучення документа з архіву вноситься до реєстраційного журналу (вказується точна дата, гриф документа та ініціали особи, яка здобула копію файлу, аналогічні дії проводяться при поверненні об'єкта);

документ, що містить комерційну таємницю, не можна виносити за межі офісу без повідомлення про це керівника департаменту безпеки;

для передачі таємних документів між філіями підприємства використовується фельд'єгерська пошта – захищена кур'єрська передача документів особливої важливості.

Акцентуємо, що за статистикою спостерігається подальше зростання загроз цифровій безпеці для власників як особистих, так і корпоративних мобільних пристроїв. Аналітики відзначають низький рівень інформаційної безпеки корпоративних користувачів навіть у випадках не самих складних атак. Число небезпечних програм лише за 2019 рік в 4 рази перевищило їх число за попередні п'ять років, а самі програми стали витонченішими і складнішими. Особливу небезпеку становлять шкідливі програми для пристроїв на основі операційної системи Android.

За відкритими даними, кількість шкідливих програм для мобільних пристроїв на основі ОС Android наблизилася до 750. Поряд із SMS-троянськими програмами особливу небезпеку для корпоративних користувачів представляють DDoS-атаки. Зросли як їх число, так і потужність та інтенсивність.

Щоб захиститися від таких загроз, недостатньо антивірусних програм, що встановлюються на мобільні пристрої. Убезпечити може тільки комплексна система забезпечення інформаційної безпеки корпоративного класу.

Одним з рішень захисту трафіку мобільних пристроїв є послуга оператора зв'язку „Мобільний VPN". У цьому випадку весь трафік мобільних пристроїв передається за закритими каналами оператора зв'язку і не потрапляє в Інтернет, що виключає ризик перехоплення нею зловмисниками.

Доцільно звернути увагу на те, що для смартфонів характерні ті ж самі загрози, що і для персональних комп'ютерів, оскільки телефон, по суті, і є комп'ютером. Це зумовлює і можливість запуску „троянських" програм, і шпигунство за власниками, і крадіжку конфіденційної інформації, крадіжку грошей з мобільних рахунків власників.

Захистити інформацію від несанкціонованого доступу можна за допомогою апаратно-програмних, програмних, біометричних, технічних і адміністративних засобів.

Існують наступні концептуальні механізми цифрової безпеки для підприємств:

ідентифікація та аутентифікація;

контроль і управління доступом;
протоколювання і аудит;
шифрування;
контроль цілісності;
екранування.

Загальний алгоритм управління ризикозахищеністю бізнес-процесів підприємств в умовах цифровізації представлено на рисунку 2.14.

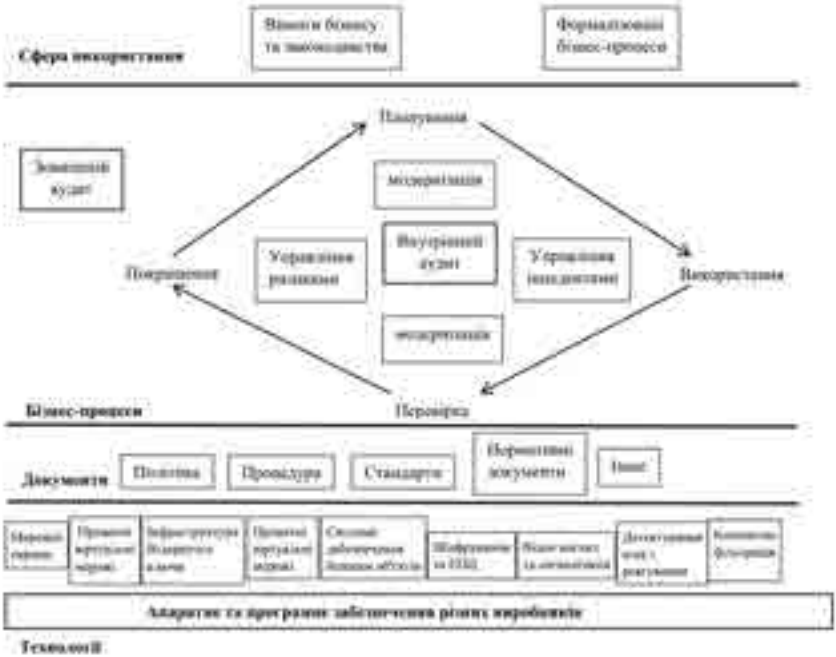


Рис. 2.14. Загальний алгоритм управління ризикозахищеністю бізнес-процесів підприємств в умовах цифровізації

Сучасні процеси цифрової трансформації економіки й пов'язані з впровадженням цифровізації підприємств й розвитком бізнес-моделей, що використовують цифрові платформи. Фактично протягом останнього десятиріччя відбувалася революція цифрових платформ.

Особливістю цифрових платформ є об'єднання різних груп споживачів, виробників, власників ресурсів на одному віртуальному майданчику.

Зростання ділової активності із застосуванням хмарних технологіях, придбання товарів через мережу Інтернет, Інтернет-банкінгу, он-лайн розрахунки сприяють зростанню економічних злочинів із застосуванням IT-технологій. Стан кіберзлочинності у світі у 2019 році представлений на рисунку 2.15.

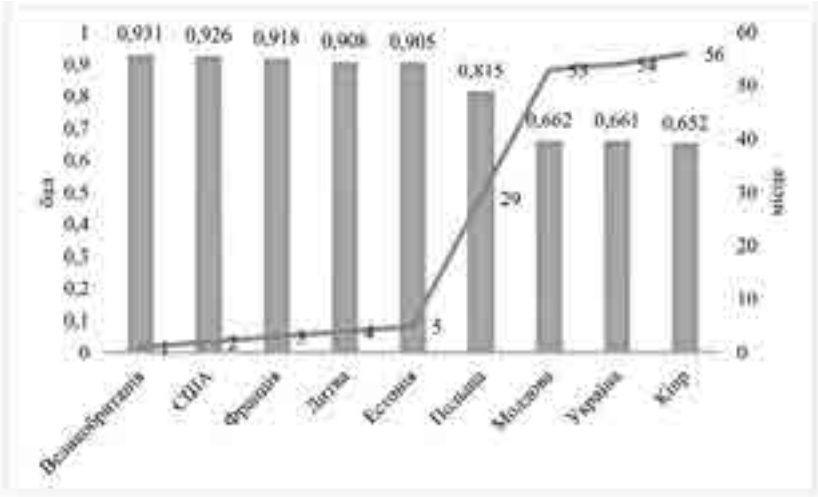


Рис. 2.15. Стан кіберзлочинності у світі у 2019 році

На рисунку 2.16. представлена інформація щодо кількості кіберзлочинів у 2015-2020 роках в Україні.

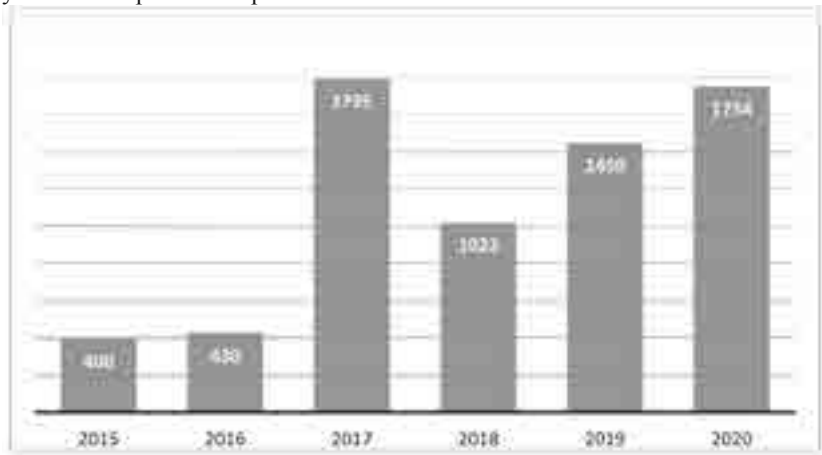


Рис. 2.16. Кількість кіберзлочинів у 2015-2020 роках

Кіберзлочин – дія, що порушує закон, який вчинено з використанням інформаційно-комунікаційних технологій та націлене на мережі, системи, інформаційний масив, веб-сайти і цифрові технології, або сприяє вчиненню злочину. Кіберзлочин відрізняється від традиційного злочину тим, що він „не визнає фізичні або географічні кордони" і може відбуватися з меншими зусиллями, більшою легкістю і з більшою швидкістю, ніж традиційні злочини

(хоча це залежить від різновидувиду кіберзлочину та традиційного злочину, з яким він порівнюється).

Коли інформаційно-комунікаційні технології є частиною способу вчинення злочину, кіберзлочинність включає в себе традиційний злочин (наприклад, шахрайство і крадіжку), вчинення якого тим чи іншим чином сприяє мережа Інтернет та цифрові технології й платформи.

При підключенні до мережі Інтернет, варто здійснювати наступні дії:

регулярно оновлювати операційну систему і встановлене програмне забезпечення;

регулярно видаляти програмне забезпечення, яке більше не використовується;

використовувати антивірусну програму, розроблену компанією з надійною репутацією;

не завантажувати програмне забезпечення, фільми або музику з сайтів загального доступу – вони часто мають шкідливу програму;

не завантажувати вкладення і не натискати на посилання від невпізнаних відправників;

не надавати особисту інформацію на невідомих веб-сайтах;

підтверджувати правильність адресу веб-сайту при введенні фінансової інформації.

Таким чином, за сучасних умов функціонування підприємств, з урахуванням існуючих трендів економічного розвитку національної економіки, особливої важливості набуває проблема захисту підприємств від негативних впливів бізнес-середовища в умовах цифровізації.

Враховуючи останні виклики й кризові процеси (масовані несанкціоновані руйнівні втручання у цифрову та комунікаційну інфраструктуру, у функціонування комп'ютерних, інфо-комунікаційних, мобільних мереж, що вип'ятили неготовність та вразливість вітчизняних підприємств та їх хиткість до ефективного протистояння потужним кібератакам), підприємства, їх партнери (замовники програмного забезпечення, користувачі ІТ-послуг) готові додатково інвестувати в безпекові системи та у захист своїх цифрових даних (впровадження антивірусних програм, апаратне забезпечення, ефективний програмно-апаратний захист, додаткові організаційні заходи, убезпечення цифрових комунікацій тощо) від деформацій, знищення, пошкодження чи викрадення, що вважаємо на часі.

У процесі управління ризиками, підприємства мають вирішувати гострі питання щодо відбору персоналу для розробки та впровадження ІТ-послуг і ІТ-продуктів, забезпечення своєчасності виконання різних цифрових проєктів, дієвих способів усунення помилок щодо формування програмних кодів, різноманітних збоїв у програмному забезпеченні тощо. Все це генерує додаткові ризики (табл. 2.6). Вибір та використання різноманітних методів управління ризиками на підприємствах в умовах цифровізації, залежить від їх фінансового стану та ресурсних можливостей. Нині, широке застосування методів управління ризиками в підприємствах поки не спостерігається і часто

зводиться до диверсифікації, страхування та формування резервів і запасів, тобто самострахування.

Таблиця 2.6

Методи управління ризиками цифровізації в підприємствах

Блок	Ризик	Методи управління ризиками	Види інструментарію
Інвестиційні ризики	Ризик розробки продукту неналежної якості	Розподіл ризиків Прогнозування та ухилення від ризикових подій Отримання фінансових гарантій Самострахування Лімітування Диверсифікація Хеджування Страхування	формування партнерських відносин, юридичні, договірні методи, формування резервів, моніторинг, контроль
	Ризик недотримання встановлених строків розробки продукту		
	Ризик перевищення бюджету витрат		
	Юридичний ризик, адміністративно-нормативні ризики		
Операційні ризики	Технологічні ризики ризики діджиталізації	Диверсифікація Страхування	Формування резервів, моніторинг, контроль
	виробничі ризики	Превенція ризиків	
	підприємницькі ризики	Диверсифікація Самострахування	
	адміністративно-нормативні ризики	Прогнозування та ухилення від ризикових подій	

Примітка: сформовано за [75].

Процес формування резервів і запасів є доволі складним, вимагає додаткового інформаційного забезпечення та аналітичної роботи. Саме тому, як правило, резервування здійснюється в межах великих підприємств [75], а малі підприємства обмежуються більш простими методами управління ризиків. Використання підприємствами ключових методів управління ризиком та оцінка їх результативності за роками продемонстрована у таблиці 2.7.

Переважно, підприємства обирають та використовують методи управління ризиками:

пасивно, тобто реакція підприємства на ризикові явища відбувається незалежно від моменту його настання або зовсім млява реакція на окремі

ризикові процеси, при цьому мало відчутний вплив спектру загроз на вибір та використання методів управління ризиками;

реактивно, тобто реакція підприємства на ризикові явища відбувається після їх настання, зовнішнє середовище вважається постійним джерелом загроз, викликів, які впливають на вибір та використання методів управління ризиками;

активно, тобто реакція підприємства на ризикові явища відбувається у момент, коли воно настає при високому впливі чинників зовнішнього середовища на вибір та використання методів управління ризиками.

Таблиця 2.7

Використання підприємствами ключових методів управління ризиком та оцінка їх результативності за роками (%).

Методи управління ризиком	2016 – 2018 рр.		2019 – 2021 рр.	
	використання методу	результативність методу	використання методу	результативність методу
Диверсифікація	56	76	78	65
Лімітування	34	34	42	42
Самострахування (формування резервів)	51	86	69	77
Превенція ризиків	26	45	34	42
Хеджування	18	23	24	32
Страхування	69	86	82	78
Отримання фінансових гарантій	17	76	26	87
Прогнозування та ухилення від ризикових подій	23	34	32	28
Розподіл ризиків (формування партнерських відносин, юридичні, договірні методи)	15	37	29	46

Примітка: сформовано за [75].

Таким чином, ключовими чинниками недосконалості системи управління ризиками підприємств в умовах цифровізації, слід вважати неадекватність та несвоєчасність вибору використання методів управління ризиками, що не дає змогу своєчасно ухвалювати відповідні управлінські заходи.

Переважно, підприємства, не мають достатнього досвіду щодо вибору та використання методів управління ризиками, водночас, наголосимо на позитивних аспектах їх практики: активне використання методів ідентифікації, діагностики та ранжування ризиків; своєчасне інформування акціонерів і партнерів про причини та обсяг можливих втрат; розробка адаптаційних заходів для пристосування до нових реалій сьогодення тощо.

На часі використання проактивних методів управління ризиками в підприємствах в умовах цифровізації.

Контрольні питання для самодіагностики по тематиці 2 модуля

1. Із якою метою здійснюють діагностику ризиків?
2. Назвіть головні джерела інформації, що використовують під час оцінювання ризиків.
3. Які є види аналізу ризиків?
4. Назвіть етапи оцінювання ризиків на підприємстві.
5. Які ви знаєте якісні методи оцінювання ризиків?
6. У чому полягає експертний метод оцінювання ризиків?
7. До якого з методів належить метод Дельфі?
8. Які показники використовують для оцінювання ризиків?
9. Що становить ідентифікація ризиків та в чому полягає її мета?
10. Розкрийте поняття „джерело ризику”.
11. Як ви розумієте поняття „небезпека”?
12. Назвіть етапи ідентифікації ризиків.
13. Що містять операційні ризики підприємства?
14. Перелічіть внутрішні джерела інформації для ідентифікації ризиків.
15. Що становить метод ідентифікації ризиків аналіз дерева подій.
16. Що становить система управління ризиками цифровізації?
17. Чим відрізняється суб’єкт управління ризиками від об’єкта?
18. Назвіть властивості, притаманні системі управління ризиками в умовах цифровізації.
19. Назвіть головні принципи системи управління ризиками в умовах цифровізації?
20. Які є види обмежень системи управління ризиками? Назвіть їхні особливості.
21. Які дії впливають на зниження інформаційного ризику?
22. Що є основним для визначення ступеня ризику цифровізації?
23. Що включає програма ризикозахищенності підприємства?
24. Охарактеризуйте методичні підходи до діагностики управління ризиками підприємств.
25. У чому полягає сутність і завдання ризикозахищенності підприємства в умовах цифровізації.
26. Дайте характеристику ризикозахищенності підприємства в умовах цифровізації.
27. Окресліть особливості управління ризиками цифровізації підприємств.
28. Назвіть джерела виникнення ризиків цифровізації.
29. У чому небезпека для підприємств кіберризиків?
30. Які дії варто здійснювати при підключенні до мережі Інтернет?
31. Охарактеризуйте стан кіберзлочинності у світі.
32. Розкрийте поняття „інформаційні ризики та „інформаційна безпека” підприємства.

МОДУЛЬ 3
ПРІОРИТЕТНІ НАПРЯМИ РОЗВИТКУ УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ

3.1. Напрями активізації розвитку управління ризиками підприємств

З'ясуємо сутність поняття „розвиток управління ризиками підприємств", оскільки, „внаслідок розвитку управління виникає новий якісний стан підприємства, що проявляється у зміні його складу або структури (тобто виникнення, трансформація або зникнення його елементів чи зв'язків) [6; 168]. Цікаво, що ще Г. Гегель стверджував, що розвиток не проходить по замкненому колу, а здійснюється поступово від нижчих до вищих форм, супроводжуючись переходом кількісних змін в якісні, і джерелом розвитку є протиріччя [26]. У наукових публікаціях знаходимо розгляд трьох ключових підходів до сутнісного тлумачення категорії „розвиток [6; 25; 138]: через вивчення і виділення властивостей систем, які розвиваються; через формування трактувань цієї дефініції; як порівняльної характеристики об'єкта" [6; 25; 138].

Системне узагальнення наукових підходів щодо визначення сутнісних ознак категорії „розвиток" продемонстровано на рисунку 3.1.

Рис. 3.1. Системне узагальнення наукових підходів до визначення сутнісних ознак категорії „розвиток"
Примітка: сформовано за [6; 25; 138].

Тобто, розвиток як закон самого буття, окреслює перехід за певною траєкторією від одного його стану до іншого, який буде характеризуватися новими кількісними та якісними властивостями. Зважаючи на швидкість трансформацій економічного простору для функціонування підприємств, слід,

окреслювати „розвиток управління” у контурі: зміни мети і завдань підприємства, нової траєкторії розвитку, адаптації до внутрішніх і зовнішніх конкурентних умов, перетворення організаційного дизайну підприємства (рис. 3.2).

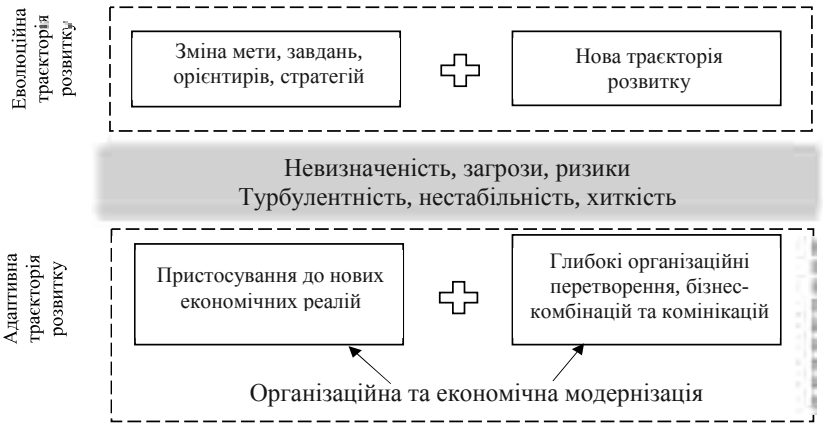


Рис. 3.2. Підходи до формування траєкторії розвитку управління ризиками
Примітка. систематизовано на основі [104, 113, 124, 125, 127, 168]

В. Шандова [168], Т. Надтока [113], Н. Мала [104], І. Підкамінний [124], Ю. Плугіна [125] погоджуються, що „розвиток управління є сукупністю змін якісного стану підприємства під впливом чинників зовнішнього та внутрішнього середовищ” і далі стверджують, що „за своєю спрямованістю розвиток може бути висхідним, спадним чи нейтральним, в залежності від стадій життєвого циклу підприємства” [127 с. 67].

Підгрунтям змістовної інтерпретації категорії „розвиток управління ризиками” доцільно визначити вимоги наступних ключових принципів: сутнісної повноти, комплексності, системної цілісності управління, синергетичності, гармонійної збалансованості управління, цільової зорієнтованості управління, органічної єдності усіх складових.

Отже, розвиток управління ризиками підприємства – це динамічний процес трансформації якісного та кількісного стану управлінської системи підприємства під впливом дії ризиків внутрішнього та зовнішнього середовища, що передбачає формування нових характеристик і властивостей управлінської системи з використанням ситуаційної адаптації до кризових умов функціонування. Нині, дослідники окреслюють декілька ключових моделей і концепцій розвитку управління ризиками підприємства (додаток). Опираючись на обґрунтування дослідників [56 с.238-240; 127 с.109-110] щодо поняття „розвиток управління ризиками” підтримуємо його розгляд у зрізі трьох ключових траєкторій (рис. 3.3).

Рис. 3.3. Траєкторії розвитку управління ризиками підприємств
Примітка: сформовано за [104, 113, 124, 125, 127, 168].

Наочно, формування унікальної траєкторії розвитку управління ризиками продемонстровано на рисунку 3.4. Означено наукові положення до формування унікальної траєкторії розвитку управління ризиками для кожного підприємства, які враховують специфіку його організаційного дизайну, обсяги діяльності, рівень діджиталізації, вплив ризикоформуючих чинників, конкретизують площини витоків загроз та ризиків, що забезпечить обґрунтованість, об'єктивність і своєчасність прийняття адекватних управлінських заходів, сприятиме пошуку стратегічних альтернатив та імплементації превентивних управлінських рішень щодо мінімізації чи уникнення ризиків.

В. Ляшенко стверджує, що „розвиток управління ризиками невід'ємно пов'язано зі змінами, але найбільшим результатом розвитку є вдосконалення та пропонує розглядати розвиток у зрізі трьох аспектів: „зміна", „зростання", „вдосконалення" [103].

Водночас, результатами розвитку управління ризиками на підприємстві, переважно дослідники визначають: „зменшення впливу зовнішнього середовища через опір, стійкість, адаптивність тощо" [82 с. 6; 128 с. 32; 130 с. 62]; „підвищення значущості підприємства" [115 с. 161]; „збільшення можливостей" [15]; „зростання ефективності функціонування" [82 с. 6; 130 с. 62].

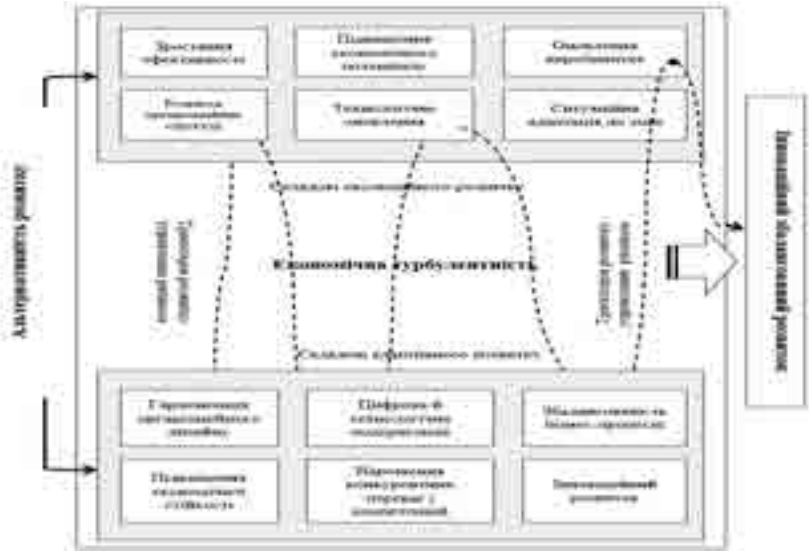


Рис. 3.4. Формування унікальної траєкторії розвитку управління ризиками підприємства
Примітка: сформовано за [104, 113, 124, 125, 127, 168].

Вирішальними передумовами, що спонукають підприємство до розвитку управління ризиками можна вважати [126 с.130; 127 с.75]:

кризові ситуації та явища в його економічній та управлінській діяльності;

унеможливлення використання існуючого стилю, методів, технології управління, які вже вичерпали себе;

трансформації у зовнішньому середовищі, що зумовлюють генерування нових загроз, викликів, ризиків, на які підприємство має своєчасно знайти адекватну відповідь;

примноження економічного потенціалу, зростання сукупності ресурсів, здатностей, компетенцій персоналу і відповідно до яких, система управління ризиками не відповідає наявним резервам та можливостям;

недосконаліть організаційних аспектів, невідповідність комунікаційних ланцюгів новим бізнес-комбінаціям та бізнес-процесам підприємства;

досягнення ліміту можливостей нарощення ефективності діяльності підприємства та продуктивності праці у контурі існуючої організаційної та управлінської системи;

трансформація цільових орієнтирів партнерів, споживачів, клієнтів підприємства;

загострення конкурентної боротьби на ринку, падіння іміджу чи конкурентоспроможності підприємства.

Формування конкурентних переваг зумовлює знаходження нових підходів до траєкторій розвитку управління ризиками на підприємстві (додатки). Останнім часом у вітчизняній та світовій економічній науці та практиці пошук напрямів активізації розвитку управління ризиками підприємств є вкрай актуальні. Цим проблемам присвячуються статті у науковій та популярній літературі, проводяться спеціальні тематичні семінари та конференції. Концептуальні підходи до активізації розвитку управління ризиками в підприємствах висвітлено в працях науковців: [151, 57, 86, 14, 146]. Методологія активізації розвитку управління ризиками підприємств у пост воєнний період має базуватися на міжнародних стандартах, відомих моделях світових компаній та науковців з врахуванням загально-управлінських, загальних принципів ризик-менеджменту та специфічних для підприємств принципів. Аналіз міжнародних стандартів управління ризиками виконано в публікаціях вітчизняних вчених [52, 30,153]. Крім того, слід враховувати такі тенденції як – обов'язковість запровадження нових цифрових рішень підприємствами; поступова та невпинна інтеграція у західноєвропейський комунікативний простір та побудова єдиного цифрового ринку з ЄС тощо. Розглянемо підходи до поняття „активізація" (табл. 3.1).

Таблиця 3.1

Підходи до трактування поняття „активація" в управлінні підприємством

Термін	Визначення
Активація (Activation) (менеджменту)	це час початку, коли повністю або частково запускається план забезпечення безперервності бізнесу (business continuity, BC), зв'язку з кризовими ситуаціями (crisis communication, CC), управлінням кризовими ситуаціями (КМ) або плану аварійного відновлення (disaster recovery, DR) [176] https://www.bcmpedia.org/wiki/Activation
Активація (загальне, в управлінні)	або активувати, дієслово – означає привести в рух; зробити активним або більш активним [187]
Активація (стратегії)	це крок з визнання того, що перед впровадженням або виконанням чогось, людей потрібно переконати в бажанні внести зміни. Активація стратегії – це те, що відбувається між створенням стратегії та виконанням стратегії [177]
Управління активацією бренду (Brand Activation Management, BAM)	це те, як підприємство організовує та використовує всі наявні ресурси, необхідні для забезпечення узгодженості, частоти та адаптивності, необхідних для досягнення визнання та вдячності споживачів, а також співробітників, потенційних новобранців та громадськості в цілому [179]
Активація (як функція)	забезпечення зацікавленості всіх учасників процесу управління та ефективності їх дій [108]
Активація (як частина мотивації)	цілеспрямований вплив на сформовану систему мотивів організаційної поведінки менеджера [2]

Примітка: систематизовано автором

Виходячи з цього, поняття «активізації розвитком управління ризиками підприємств», визначено як «*цілеспрямований вплив на розвиток управління ризиками підприємств з виключення або зниження негативних наслідків настання ризикових подій для прискорення досягнення підприємством стратегічної мети та завдань бізнес-комбінацій, процесів розвитку та підтримки*».

До основних напрямів активізації розвитку управління ризиками підприємств можна віднести:

1. Усвідомлення ризиків та їх загроз для досягнення мети функціонування підприємства та їх подальша ідентифікація (ідентифікація активів, ідентифікація джерел ризиків, ідентифікація ризикових подій, ідентифікація заходів контролю, ідентифікація наслідків).

2. Формулювання змісту декларації та настанов з ризик-менеджменту. У самому спрощеному вигляді декларація відображає філософію телекомунікаційного підприємства щодо управління ризиками (відношення організації до ризиків; розмежування повноважень між суб'єктами ризик-менеджменту; персоналізація відповідальності тощо). Декларація містить викладення мети, завдань та принципів управління ризиками, а також опис методів ризик-менеджменту, використання яких суб'єктами управління є припустимим (наприклад: зниження можливості виникнення аварій; формування стабілізаційних (резервних) фондів для фінансування можливих втрат; страхування тощо) [112 с.62].

3. Формування організаційної структури управління ризиками та формалізація її діяльності (положення про структурний відділ, інструкції, плани тощо).

4. Визначення принципів управління ризиками (принципи можуть бути закріплені в окремому документі або бути зафіксовані в декларації з ризик-менеджменту). Незалежно від форми формалізації (оформлення) принципів їх зміст повинен бути пов'язаний з механізмами управління ризиками.

Основні напрями активізації управління ризиками підприємств які можна представити у вигляді трикутника взаємопов'язані між собою, охоплюють стадії процесу управління ризиками, співвідносяться до функцій менеджменту та є базою механізму управління ризиками телекомунікаційного підприємства (рис. 3.5). Базисом трикутника напрямів активізації розвитку управління ризиками підприємств вважаємо визначення принципів управління ризиками підприємства. Ефективний і життєздатний розвиток управління ризиками підприємств повинен відповідати системі принципів, яка враховує загальні принципи управління ризиком та специфічні принципи ризик-менеджменту самих підприємств.

Принципи управління ризиками відображують:

1) розмежування повноважень (права, обов'язки, відповідальність) між суб'єктами ризик-менеджменту, а також визначення організаційної ієрархії;

2) порядок отримання інформації про ризики та умови їх позиціонування (динаміка надходження та особливості розподілу між суб'єктами управління);

3) особливості взаємодії між суб'єктами та об'єктами ризик-менеджменту, а також порядок взаємодії з основними партнерами організації;

4) дії при загостренні ризикової ситуації;

5) зміст підходів до управління ризиками, а також пріоритетність використання тих чи інших методів (механізмів) управління ризиками;

6) контроль за процесом та результатами управління [112 с.69].

Рис. 3.5. Трикутник напрямів активізації управління ризиками підприємств
Примітка: розроблено на основі [2, 36, 37, 44, 89].

Загальні принципи управління на підприємстві наведено у додатку. Фактично, принципи управління ризиком в підприємствах можна розділити на три основні групи. Принципи, що входять до складу першої групи, є загальними, що відносяться до системи управління в цілому. У другій групі об'єднуються приватні принципи, що стосуються окремих частин і елементів системи управління. Принципи, складові третьої групу, регламентують порядок і правила управління конкретними видами діяльності або явищами (зокрема – ризиками).

Принципи ризик-менеджменту – спеціальні принципи, що регламентують порядок і правила управління ризиками [144 с.26]. У вітчизняному законодавстві відсутні нормативні документи, що встановлюють регламент розробки та застосування системи управління ризиками в підприємствах. В результаті підприємства, самостійно формують концепцію побудови системи управління ризиками, спираючись у цій роботі на відомі світові стандарти, що містять найкращі практики. Насамперед це стандарт ISO/IEC Guide 73 „Управління ризиками – словник – настанови по використанню у стандартах" від 2002 та 2009 років [54]; цікавим вважаємо

стандарт управління ризиками, що розроблений в COSO (The Committee of Sponsoring Organizations of the Treadway Commission), а саме модель COSO ERM (Enterprise Risk Management) [119, 182, 193] (додаток), розроблений у 2004 році. У Європі широкого поширення набули стандарти управління ризиками FERMA [175, 192], створені в 2002 році Інститутом ризик-менеджменту (IRM) та Асоціацією ризик-менеджменту та страхування (AIRMIC) (додаток) . Слід також згадати ISO 31000:2009 [120] та ISO 31000:2018 [179, 53] „Управління ризиками. Принципи та рекомендації", розроблений та доповнений Міжнародною організацією зі стандартизації (International Organization for Standardization), а також ISO/TR 31004:2013 „Управління ризиками – Керівництво з впровадження ISO 31000м" [55]. У роботі О.М. Донець, Т.В. Савельєвої, Ю.І. Урецької висвітлено важливість впровадження міжнародних стандартів в управлінні ризиками проектно-орієнтованих підприємств, розроблено напрями та алгоритм опису ризиків на основі вимог провідних міжнародних стандартів з ризик-менеджменту [52]. У публікації Т.В. Головач, А.Б. Грушевицької, В.В. Швид досліджено теоретичні та практичні питання застосування ризик-менеджменту на підприємствах, функції та основні етапи ризик-менеджменту, основні міжнародні стандарти ризик-менеджменту [30]. Н. Стрельбіцька досліджує міжнародний стандарт управління ризиками ISO 31000: 2009, розглядає взаємозв'язок між принципами, системою і процесом управління ризиками та зміни у термінологічній базі [153].

Всі ці стандарти та рекомендації мало відрізняються, у них не розглядається специфіка бізнесу, але доступно та чітко виражаються основні поняття управління ризиками, ідеологія процесу управління та бажані стадії розробки та функціонування. Також, нажаль, лише декілька міжнародних стандартів виділяють принципи управління ризиками, якими слід керуватися для активізації розвитку управління ризиками в підприємствах (табл. 3.2).

Визначення сутності ризику та управління ним висвітлено в деяких нормативно-законодавчих актах України [131, 132, 133, 134, 135], але вони не містять перелік принципів, якими слід керуватися при активізації системи управління ризиками на підприємстві. В Україні принципи управління ризиками зафіксовані у «Положенні про організацію системи управління ризиками в надавачах фінансових послуг та небанківських фінансових групах» [136], де описані основні положення ризик-менеджменту, створення комплексної, адекватної та ефективної системи ризик-менеджменту з урахуванням особливостей фінансової діяльності, характеру, обсягів фінансових операцій, профілю ризиків та системної важливості фінансових установ, яка відповідає таким принципам: ефективність; своєчасність; структурованість; розподіл обов'язків; усебічність та комплексність; пропорційність; незалежність; конфіденційність; прозорість [136]. Підходи до принципів управління ризиками на підприємствах, наведені в працях вітчизняних науковців [86 с.60; 146, с.46-47; 147 с.17; 14 с.27; 112 с.63; 27 с.166-168] (додаток).

Таблиця 3.2

Принципи управління ризиками за міжнародними стандартами

Номер стандарту	Назва стандарту (англ.)	Назва стандарту (укр.)	Рік	Організація-розробник	Сутність стандарту	Принципи згідно із стандартом
COSO II ERM – Integrated Framework [119] COSO ERM [182 с.3]	Enterprise Risk Management – Integrated Framework. Enterprise Risk Managament – Integrating with Strategy and Perfomance	Інтегрована модель управління ризиками підприємства. Управління ризиками підприємства – інтеграція зі стратегією та продуктивністю	2004 2016 2016	Комітет організацій-спонсорів Комісії Тредвея (The Committee of Sponsoring Organizations of the Treadway) США	Цей документ описує концептуальні основи управління ризиками підприємств, в якому міститься детальна інформація та рекомендації стосовно створення корпоративної системи ризик-менеджменту в рамках підприємства.	Виділяє шість принципів: 1) пропорційні процедури; 2) зобов'язання на найвищому рівні; 3) оцінка ризику; 4) належна обачність; 5) спілкування (включаючи навчання); 6) моніторинг та огляд. Принципи є базою структуру COSO ERM, яка складається з п'яти взаємопов'язаних компонентів: управління та культура; стратегія та постановка цілей; продуктивність; огляд і перегляд; інформація, комунікація та звітність
ISO 31000:2009 [120] ISO 31000:2018 [53]	Risk management – Principles and guidelines on Implementation	Управління ризиками. Принципи та рекомендації	2009 2018	Міжнародна організація зі стандартизації (International Organization for Standardization)	Основний стандарт з ризик-менеджменту. Містить принципи та загальні вказівки з виявлення ризиків та ефективного управління ними. Даний стандарт дає загальне розуміння того, як розробити, впровадити і підтримувати ефективну систему управління ризиками в рамках галузі, підприємства тощо	1) інтегрованість; 2) структурованість і комплексність; 3) індивідуальність; (адаптованість та пропорційність зовнішньому та внутрішньому контексту організації); 4) залученість (своєчасне залучення зацікавлених сторін призводить до покращення обізнаності та інформованого управління ризиками); 5) динамічність; 6) доступність інформації; 7) людські та культурні чинники; 8) постійне вдосконалення
ISO/TR 31004:2013 [55 с.10-20]	Risk management – Guidance for the implementation of ISO 31000	Управлння ризиками – Керівництво з впровадження ISO 31000м	2013	Міжнародна Організація зі Стандартизації (International Organization for Standardization (ISO))	Цей стандарт сприяє ефективному впровадженню ISO 31000, а також забезпечує: структурований підхід до переходу від існуючої практики управління ризиками до стандарту ISO 31000 з гнучкою перспективою адаптації до майбутніх змін; роз'яснення базових концепцій ISO 31000 з рекомендаціями та прикладами, 119 адаптованими до індивідуальних потреб користувачів; додаткове керівництво за принципами ISO 31000 та основи управління ризиками.	1) управління ризиками створює та захищає вартість; 2) управління ризиками є невід'ємною частиною всіх організаційних процесів; 3) управління ризиками є частиною прийняття рішень; 4) управління ризиками чітко звертається до невизначеності; 5) управління ризиками є системним, структурованим і своєчасним; 6) управління ризиками базується на найкращій наявній інформації; 7) управління ризиками адаптивне; 8) управління ризиками враховує людські та культурні чинники; 9) управління ризиками є прозорим та інклюзивним; управління ризиками є динамічним, повторюваним і реагує на зміни; 10) управління ризиками сприяє постійному вдосконаленню організації

Примітка: *складено на основі [119; 182 с.3; 120, 53; 55 с.10-20]*

Опираючись на вказані дослідження, можна стверджувати, що до найбільш важливих загальних принципів розвитку управління ризиками підприємств слід віднести:

1. *Принцип інтегрованості* передбачає розгляд управління ризиками як невід'ємної частини діяльності підприємства, який застосовується двома методами: при розробці моделі управління ризиками (включаючи підтримку в робочому стані та його поліпшення); під час реалізації процесу управління ризиками у прийнятті рішень і пов'язаної з цим діяльності.

2. *Принцип структурованості та комплексності* сприяє досягненню погоджених і співставних результатів. Послідовний підхід до управління ризиками під час прийняття рішень дає можливість підвищити ефективність діяльності підприємства та забезпечити результати, які можуть закріпити довіру до підприємства та її успіх. Принцип структурованості передбачає чіткий розподіл функцій, обов'язків і повноважень з управління ризиками між усіма структурними підрозділами та працівниками підприємства, та їх відповідальність згідно з таким розподілом. Комплексність означає охоплення всіх видів діяльності підприємства на всіх організаційних рівнях та у всіх його структурних підрозділах, оцінка взаємного впливу ризиків. Для досягнення підприємством таких результатів необхідно, щоб у практичній діяльності всередині підприємства було закріплено врахування ризиків, які пов'язані з рішеннями, а також використання узгоджених критеріїв ризику.

3. *Принцип ефективності* означає процес управління, що забезпечує об'єктивну оцінку розміру ризиків підприємства та повноту заходів щодо управління ризиками з оптимальним використанням фінансових ресурсів, персоналу та інформаційних систем підприємства.

4. *Принцип незалежності* передбачає свободу від обставин, що становлять загрозу для неупередженого виконання підрозділом з управління ризиками та підрозділом контролю за дотриманням норм своїх функцій. Незалежність передбачає недопущення ситуації, коли винагорода працівників підрозділу з управління ризиками та підрозділу контролю за дотриманням норм, у тому числі їх керівників, пов'язана з фінансовими результатами бізнес-підрозділів.

5. *Принцип адекватної реакції та розумного прийняття* полягає у швидкій та ефективній реакції на зовнішні зміни в ризиковій ситуації, а також у прийнятті ризику лише у випадку його обґрунтованої необхідності.

6. *Принцип адаптованості* виражається через адаптацію моделі та процесу управління ризиками та відповідає зовнішньому та внутрішньому контексту підприємства, пов'язаний з його цілями. Кожен процес в управлінні ризиками необхідно адаптувати до його конкретної цілі. Структура і процес управління ризиками співвідносяться та налаштовуються з урахуванням зовнішнього і внутрішнього контексту організації, пов'язаного з її завданнями, цілями та політиками [27 с.167]. Адаптація необхідна для досягнення інтеграції з процесами прийняття рішень на підприємстві. Такі процеси прийняття рішень

можливо буде необхідно змінити для приведення у відповідність зі структурованою моделлю управління ризиками.

7. *Принцип інклюзивності* передбачає належну та своєчасну залученість стейкхолдерів, що, в свою чергу, дозволяє враховувати їх знання, думку, а це призводить до підвищення освіченості та поінформованості щодо управління ризиками. Впроваджуючи цей принцип слід враховувати конфіденційність, безпеку та секретність. Наприклад, це може виражатись у обмеженні доступу до певної категорії документації. Дуже важливим аспектом при впровадженні принципу інклюзивності є його ефективність, саме на цьому етапі можна як вибудувати, так і зруйнувати довіру стейкхолдерів. Вони обов'язково повинні бути залучені у всі аспекти процесу управління ризиками.

8. *Принцип динамічності* полягає у наявності зміни ризиків в залежності внутрішнього та зовнішнього середовища самого підприємства. Управління ризиками дає змогу вчасно передбачати, виявляти й відповідно реагувати на зміни й події. Слід проводити моніторинг, відповідний аналіз та контроль прийняття управлінських рішень.

9. *Принцип доступності, надійності та релевантності інформації* означає, що вхідні дані для управління ризиками базуються на історичній та поточній інформації, а також на майбутніх очікуваннях та прогнозах. Особливу увагу в управлінні ризиками слід приділяти невизначеності та обмеженням, що пов'язані з інформацією та очікуваннями. Надійність та точність інформації необхідно постійно перевіряти на актуальність, своєчасність та надійність.

10. *Принцип врахування людських та культурних чинників* передбачає існування впливу на всі аспекти управління ризиками на кожному рівні й етапі людської поведінки й культури. Особливу увагу слід приділити здатності знаходити та реагувати на своєчасні попередження, надмірна увага чи байдужість до думок інших або нестача знань; упередженість через спрощені стратегії обробки інформації для вирішення складних завдань.

11. Принцип постійного вдосконалення та результативності базується на розумінні та необхідності постійного покращення процесу управління ризиками на основі накопичення досвіду та постійного навчання. Постійне покращення передбачає покращення інтеграції діяльності з управління ризиками в усі види діяльності підприємства; підвищення якості оцінювання ризиків; удосконалення моделі, наприклад, якості та доступу до інформації; покращення швидкості прийняття рішень.

До принципів, які притаманні й особливо важливі слід також виділити: модульність, багатокритеріальність оцінки, індивідуальність, своєчасність, конфіденційність, прозорість (табл. 3.3). Виходячи з цього, розглянемо систему принципів з урахуванням специфіки цифровізації підприємств, яка включає *загально-управлінські*, *загальні принципи ризик-менеджменту* та додаткові *специфічні для цифровізації підприємств принципи*, використання який сприятиме активізації управління ризиками (рис. 3.6). Нині, успіх активізації розвитку управління ризиками багато в чому залежатиме від рівня зрілості підприємства, ступеня підтримки керівництва та кваліфікації персоналу.

Таблиця 3.3

Додаткові специфічні принципи управліннями ризиками підприємств в умовах цифровізації

Принцип	Характеристика принципу
Принцип модульності	тобто, можливість використання різних поєднань процедур управління ризиком підприємства у різних цифрових ситуаціях, що дозволяє врахувати специфіку конкретної ситуації та за необхідності налаштувати зазначену систему на вирішення індивідуальних потреб користувачів послуг
Принцип багато-критеріальності оцінки	різнорідність складу системи та наявність специфічних бізнес процесів (операційних, процесів розвитку та підтримки) підприємства, зокрема, означає, що кожен процес цифровізації оцінюється з різних точок зору за унікальними критеріями, у тому числі й неформалізованими, що спричиняє виникнення додаткових складнощів при аналізі процесу прийняття рішень у сфері управління ризиком
Принцип індивідуальності	Урахування специфіки цифровізації підприємств, розмірів, стадій життєвого циклу підприємств та інших чинників, які визначатимуть вплив ризику на цифровізацію бізнес-процесів
Принцип своєчасності	процес управління ризиками, що забезпечує своєчасне (на ранній стадії) виявлення, вимірювання, моніторинг, контроль, звітування та пом'якшення усіх видів ризиків цифровізації на всіх організаційних рівнях
Принцип конфіденційності, безпеки та секретності	недопущення отримання інформації, що не підлягає оприлюдненню, особами, у яких немає повноважень на її отримання, управління ризиками не порушуючи політику конфіденційності підприємства
Принцип прозорості	оприлюднення підприємством достатньої інформації щодо системи управління ризиками та профілю ризику
Принцип максимізації (масштабність) та мінімізації	максимізація полягає у прагненні до врахування якомога більшої кількості сфер можливого виникнення ризиків цифровізації на підприємстві, а мінімізація. – у зменшенні спектра проявів ризиків цифровізації і ступеня їх впливу
Принцип пропорційності	створення ефективної системи управління ризиками, що відповідає бізнес-моделі підприємства, його системній важливості, а також рівню складності цифрових операцій, що здійснюються підприємством.

Активізація розвитку управління ризиками має бути центральним елементом стратегічного управління підприємства, яка базується на дотриманні *загально-управлінських*, *принципів ризик-менеджменту* та *специфічних принципів*, що сприятиме створенню нової філософії та культури ведення бізнесу та активізації розвитку управління ризиками задля досягнення підприємством поставленої мети.

Нині, кризові деформації економічного простору, зумовлені воєнним станом, постковідними явищами, глобалізаційними й інтеграційними процесами пояснюють необхідність докорінних якісних перетворень щодо активізації розвитку управління ризиками підприємств.

Рис. 3.6. Система принципів управління ризиками підприємств
Примітка: розроблено автором

Сьогодні до загальних труднощів підприємств, додалися кадрові проблеми, пов'язані з залученням компетентного персоналу на військову службу, міграцією спеціалістів жінок за кордон; руйнування і розкрадання ворогом приміщень та обладнання тощо. Для того, щоб вистояти у ці непрості часи, підприємства, шукають і опробовують нові стратегії, технології, інструменти, методи управління ризиками що передбачають: гармонізацію організаційного дизайну, оптимізацію бізнес-процесів, зростання ринкової частки за рахунок злиття чи поглинання з іншими підприємствами, підвищення якості та розширення спектру послуг, входження до світових ринків, вдосконалення інформаційних і комунікаційних управлінських ланцюгів тощо.

Проте, вітчизняні реалії сьогодення унеможливлюють це завдання, оскільки, більшість підприємств, опираються на застарілу фрагментарну концепцію розбудови системи управління ризиками, яка ґрунтується на пасивній чи реактивній основі, опираються на інтуїтивне управління ризиками. В додатку наведено характеристику різних концепцій. Цікаво, що

зарубіжні підприємства здійснюють безперервне управління ризиками на превентивній, антисипативній основі за слабкими сигналами загроз. Настання відчутних змін в динамічному середовищі підприємства теж відбувається не водночас, фактично перед такими змінам завжди проявляються сигнали раннього попередження, слабкі сигнали. Адекватна ідентифікація яких може завчасно попередити про загрози та ризики, що наближаються. Тому, на часі, формування нової парадигми антисипативного управління ризиками в підприємствах, яка передбачає перехід від невизначеності до зрілості й гнучкості що базується на вище обґрунтованих принципах й враховує „слабкі сигнали". І. Ансоф [3] трактує слабкий сигнал, як „один із інструментів управління", вказуючи, що „це ранній сигнал, який важко відмітний від природних або нав'язаних шумів, можливо несе в собі ознаки настання важливих подій, а можливо й ні [3]. Тобто він окреслює слабкий сигнал як особливий інструмент управління невизначеностями.

Мельник О. Г., Адамів М. Є. наголошують, що, „управління по слабких сигналах можна сприймати як механізм попередньої адаптації до середовища або як антисипативне управління" [106]. Акцентуємо, що нові наукові підходи до формування управління ризиками мають будуватись на підґрунті передбачення, прогнозування настання різноманітних ризикових явищ, що зумовлюють зміни, тобто на підґрунті антиципації.

„Антисипація" у дослівному перекладі з латини (anticipatio) означає – передбачення, уявлення предмета або явища в свідомості людини до того, як вони на практиці будуть сприйняті або реалізовані" [12]. У наявних наукових та спеціалізованих виданнях знаходимо близькі до окресленого вище поняття антиципація, розглянемо їх.

„Антисипація – це: передбачення, випередження, завчасне розпізнавання можливого розвитку подій; передчасне настання будь-якого явища, яке повинне настати пізніше" [85]. „Антисипація – це: передчуття, передбачення, сподівання, побоювання; передчасність наступу" [96]. „Антисипація – це: здатність людини уявити собі можливий результат дії до його здійснення, а також можливість його мислення уявити спосіб вирішення проблеми до того, як вона реально буде вирішена (інтуїція); здатність організму людини або тварини підготуватися до реакції на будь-яку подію до його настання" [1]. „Антисипація – це передчуття, передбачення, сподівання, короткочасне прогнозування розвитку подій в майбутньому" [8]. „Антисипація – це: передбачення, здогад, прогноз; передчасне настання якогось явища, дії; заздалегідь складене уявлення про що-небудь" [16]. „Антисипація – це: завчасна дія, яка бере до уваги чи передбачає подію, що відбудеться пізніше; погляд вперед; використання безготівкових грошей (які ще не є доступними); візуалізація майбутньої події; об'єкт або форма, що передбачає подальші явища; раннє звучання одного чи декількох тонів подальшого акорду, що формують тимчасовий дисонанс" [191]. „Антисипація – це: передбачення можливого розвитку подій; передчасне настання певного явища" [59]. Тобто, переважно дослідники, антисипацію визначають, як

проактивну дію з розпізнання, передбачення, прогнозування та превентивного попередження настання певних процесів, подій, явищ. Відповідно антисипативне управління ризиками має передбачати і попереджувати настання кризових процесів, подій та ризикових явищ за ідентифікацією слабких сигналів.

Р.А. Руденський [142] характеризує антисипативне управління як „управління, що базується на таких станах елементів складної системи і зовнішнього середовища, які ще не відбулися, але очікуються, що дозволяє підвищити рівень підготовки системи управління складним економічним об'єктом до появи і розвитку неочікуваних подій, як кризового характеру, так і зв'язаних з новими можливостями" [142].

В унісон такій характеристиці В.В. Прохорова стверджує [137], що „антисипативне управління передбачає раннє розпізнавання загроз середовища функціонування та розроблення випереджувальних управлінських дій щодо їхньої локалізації з метою забезпечення стійкого розвитку підприємства [137].

Опираючись на здійснений розгляд існуючих трактувань понять „антисипація" й „антисипативне управління", визначимо антисипативне управлінням ризиками підприємств, як проактивний процес передбачення, прогнозування, сканування, розпізнання, обробки, ітерації та ідентифікації різноманітних сигналів щодо настання кризових процесів, подій та ризикових явищ що забезпечує гнучкість превентивного попередження їх впливу на основі збалансованості управлінських рішень та заходів щодо своєчасного нівелювання та мінімізації ризиків. Таке тлумачення дає змогу адекватно сформувати дієвий методичний інструментарій антисипативного управлінням ризиками підприємств, конкретизувати джерела й площини витоків загроз та ризиків, ідентифікувати й оцінити потужність їх впливу, що забезпечить обґрунтованість, об'єктивність, адекватність і своєчасність ухвалення необхідних управлінських рішень і стратегій, сприятиме пошуку альтернативних сценаріїв ризикозахищенності та імплементації результативних заходів стосовно нівелювання чи мінімізації ризиків.

Тарасова Г.О. [155] засвідчує, що „застосування методу сканування в якості основного для проведення діагностики слабких сигналів, дозволяє завчасно виявити кризу, що насувається − початкове економічне явище, яке свідчить про те, що з'явилися ознаки зміни стану організації або зовнішнього середовища підприємства" [155]. І далі умотивовується „проведення діагностики за кількісною оцінкою інтенсивності сигналів, що дає можливість визначити цю інтенсивність (потужність, діапазон) на основі доступної інформації, виділення з „фонових шумів" істинного сигналу" [155].

М.М. Рубанов [141] обґрунтовує доцільність „використання системи раннього попередження загроз за слабкими сигналами, що має ґрунтуватись на трирівневій системі контролю, що включає попередній, поточний і заключний контроль. Кожен з даних видів контролю є своєрідним бар'єром, що дозволяє попередити виникнення відхилень, здатних істотно вплинути на

підприємство, що, в свою чергу, дозволяє зробити висновок про доцільність застосування даної системи на практиці [141].

Варто виділити наступні характерні конститутивні атрибути антисипативного управління ризиками підприємств:

превентивність: спрямована на випередження дії будь-яких потенційних ризикових явищ через своєчасне ухвалення та реалізацію відповідних управлінських рішень;

систематичність: здійснюється постійно задля забезпечення високого рівня готовності підприємства до потенційних деформацій внутрішнього та коливань зовнішнього середовища у будь-який часовий період;

стратегічна зорієнтованість: цілеспрямованість на досягнення визначеної мети підприємства та стратегічних завдань, пов'язана із подоланням, мінімізацією, нівелюванням потенційних ризиків на основі максимального використання ресурсних та інших можливостей підприємства;

функціональність: здійснює розпізнавальну, попереджувальну, захисну, прогнозну, експертну, реагуючу, спостережну, інформаційну, превентивну функції задля підвищення результативності управління ризиками підприємства;

комплексність: передбачає розробку портфеля альтернативних сценаріїв розвитку ризикових процесів задля забезпечення максимальної готовності підприємства до кожного із сценаріїв;

відкритість: постійно сканує усі слабкі та латентні сигнали зовнішнього та внутрішнім середовища підприємства через сформовані інформаційні та комунікаційні прямі та зворотні ланцюги задля виявлення загроз і ризиків;

адаптивність: швидко, безболісно та своєчасно пристосовується до деформацій внутрішнього та коливань зовнішнього середовища у будь-який часовий період;

всеосяжність: спрямоване на сканування та розпізнання усіх можливих слабких та латентних сигналів зовнішнього та внутрішнім середовища щодо потенційних деформацій внутрішнього та коливань зовнішнього середовища та охоплює усі бізнес-процеси та бізнес-комбінації підприємства для виявлення загроз, ризиків та ресурсних можливостей у будь-який часовий період;

адекватність: ухвалення управлінських рішень відбувається відповідно до виявлених загроз, ризиків та ресурсних можливостей на основі моделювання та прогнозування;

пріоритетність: здійснюється ранжування виявлених загроз, ризиків та ресурсних можливостей за ступенем їх вагомості, терміновості, інтенсивності й потужності впливу на функціонування підприємства та відповідно до розроблених стратегій.

Метою формування і впровадження антисипативного управління ризиками підприємств варто визначити: удосконалення та активізація розвитку управління ризиками на основі високого рівня готовності підприємства до потенційних деформацій внутрішнього та коливань

зовнішнього середовища у будь-який часовий період для забезпечення стабільності стратегічного розвитку підприємства за допомогою розробки і ухвалення збалансованих управлінських заходів зорієнтованих на превентивне подолання, нівелювання чи мінімізацію ризиків через максимальне використання ресурсних можливостей підприємства.

Відповідно до мети антисипативного управління ризиками підприємств окреслимо його ключові завдання:

своєчасна безболісна адаптація підприємства до нових викликів та реалій сьогодення;

ухвалення та реалізація превентивних рішень щодо реагування на трансформації, що передбачаються в перспективі;

максимально результативне опрацювання від зайвого шуму усіх можливих слабких та латентних сигналів щодо потенційних деформацій внутрішнього та коливань зовнішнього середовища тощо.

Ключовими перевагами формування та впровадження антисипативного управління ризиками підприємств можна визначити:

підприємство має можливість заздалегідь розробити адекватні рішення до того, як загрози та ризики наберуть обертів та потужного впливу і своєчасно сформувати резерви та запаси для вирішення гострих проблем та реалізації нових можливостей;

технології антисипативного управління ризиками за слабких та латентних сигналів сприяють моніторингу, експертизі, ідентифікації, діагностиці і розробці адекватних реакцій підприємства на деформації внутрішнього та коливання зовнішнього середовища, нові реалії та виклики сьогодення;

можливість трансляції підприємством, деяких сильних, слабких чи латентних сигналів в оточення для інформування усіх контактних аудиторій;

формування адекватного гнучкого гармонійного організаційного дизайну підприємства;

розвиток компетентностей працівників підприємства та підвищення їх креативності.

На багатьох підприємствах, управління ризиками носить фрагментарний, досить поверховий характер. Одна із основних причин, що заважають розвитку управління ризиками в них, полягає в тому, що у керівництва підприємств немає ясного уявлення про механізм такого розвитку, не кажучи вже про переваги від модернізації цього механізму із запровадженням контрольно-дозвільної комплаєнс-функції та проактивних методів управління, що притаманні управлінню ризиками на підґрунті антиципації та інтеграції цього механізму в загальну систему управління.

Варто зазначити, що більшість ризиків та загроз є уніфікованими та повторюваними, вони виникають через об'єктивні чи суб'єктивні чинники впливу, саме тому менеджмент підприємства має розробляти конкретні чіткі правила реагування на будь-яку відому чи не відому ризикову ситуацію.

Акцентуємо, що комплаєнс-ризики становлять велику небезпеку, оскільки можуть генерувати для підприємства події, пов'язані з великими

збитками. Комплаєнс (англ. compliance − відповідність) − це здатність підприємства відповідати нормам та правилам, як зовнішнім, так і внутрішнім. Бути відповідальним за ведення бізнесу [173]. Комплаєнс-ризики можуть вести до репутаційних втрат, що зумовлює втрату частини ринку, ділової репутації тощо. І тому, запровадження контрольно-дозвільної комплаєнс-функції набуває ключового значення у контурі інтеграції системи управління ризиками підприємств в загальну систему управління має бути присутнім на всіх ієрархічних рівнях.

Нині, загальноприйнятою точкою зору є, те що комплаєнс-ризики генеруються, внаслідок виникнення різних форм конфлікту інтересів різних контактних аудиторій підприємства (від топ-менеджменту до рядових виконавців), що призводить до невідповідності їх дій різним регламентам і нормативним документам, а також правовим зобов'язанням.

Практична реалізація контрольно-дозвільної комплаєнс-функції в сучасних підприємствах полягає у включенні контрольних елементів (контрольних точок) в основні бізнес-процеси. Тому комплаєнс-функцію у процесі інтеграції управління ризиками можливо поєднати з будь-якими бізнес-процесами підприємства. Фактично, комплаєнс може розглядати як сучасну концепцію здійснення контрольно-дозвільної функції управління ризиками на основі документально зафіксованих регламентів бізнес-процесів (у тому числі, цифрових процесів й операцій) і проектів. І, у цьому відношенні, він має високий потенціал застосування як елемент механізму розвитку управління ризиками. Особливо, в частині ризиків, пов'язаних з поведінкою персоналу, та його конфлікту інтересів.

Враховуючи те, що здійснення контрольно-дозвільної комплаєнс-функції будується навколо ризиків конфлікту інтересів персоналу підприємства, ідентифікуємо види подібних конфліктів залежно від рівня регулюючих документів (регламентно-нормативної системи) з порушенням, яким пов'язані відповідні комплаєнс-ризики.

Базовим різновидом конфлікту інтересів стейк-холдерів різного рівня, що веде до виникнення комплаєнс-ризиків, і, відповідно, ризиків цифровізації, є, загалом, конфлікт (суперечність) інтересів безпеки та інтересів отримання матеріальної вигоди різних стейк-холдерів у середньостроковій та короткостроковій перспективі. При довгостроковому плануванні суперечності між безпекою та вигодою не виникає через те, що збігаються інтереси стейк-холдерів: акціонерів, власників, інвесторів, а також суспільства в цілому. Тобто, матеріальна вигода збігається з альтернативою забезпечення безпеки, збереження майна, цінностей, а також відсутності шкоди для зовнішніх сторін, яка пов'язана із суттєвими втратами на відшкодування завданої шкоди, репутаційними витратами.

Реалізація даних протиріч, як правило, може виражатися в наступних формах:

1) Конфлікту інтересів безпосередніх виконавців, що призводить до суперечності бізнес-практик (бізнес-процесів та поведінки окремих виконавців) стандартам і регламентним нормам управління підприємства, що

веде до зниження технічної безпеки (ризики поведінкового та виконавчого комплаєнсу персоналу). При цьому, можна відзначити наявність конфлікту інтересів, що веде до виникнення комплаєнс – ризиків: коли порушення регламентуючих документів здійснюються на користь отримання матеріальної вигоди безпосереднім виконавцем (це може статися при порушенні техніки безпеки при виконанні робіт з метою підвищення продуктивності, скорочення часу виконання операції, порушення технічних умов і стандартів операцій тощо).

2) Конфлікту інтересів операційного менеджменту, коли керівники, з метою отримання власної вигоди (як правило, досягнення власних високих оцінок ефективності − KPI та інших, з отриманням відповідного матеріального чи нематеріального, наприклад, підвищення за посадою заохочення) примушує нижчестоящих працівників до порушення регламентів здійснення операцій, бізнес-процесів та регулюючого законодавства (зазначимо, що конфлікти інтересів цього роду вступають у протиріччя з інтересом решти стейк-холдерів підприємства: топ-менеджменту, власників, інвесторів, акціонерів, держави й суспільства).

3) Конфлікту інтересів вищого менеджменту, внаслідок чого, як правило, може виникати протиріччя стандартів і регламентів (регламенти технологічних та бізнес-процесів, регламенти роботи, технічні умови тощо) управління підприємством із системою технічного регулювання та законодавства. Метою подібних порушень є підвищення показників ефективності підприємства (прибуток, виручка, обсяг виробництва) за рахунок ігнорування вимог технічної безпеки, природоохоронного законодавства, нормативів щодо захисту здоров'я та природних ресурсів. В даному випадку, інтереси власної вигоди вищого менеджменту (в результаті отримання особистої матеріальної та нематеріальної винагороди за високі операційні та фінансово-економічні результати підприємства) протиставляються інтересам власне підприємства, його акціонерам чи власникам, інвесторам, а часто й інтересам безпосередніх виконавців.

4) Конфлікту інтересів підприємства законним інтересам його контрагентів, протиріччя діяльності підприємства його правовим зобов'язанням (у тому числі цивільно-правовим), а також законним інтересам третіх осіб та організацій (цивільно-правові комплаєнс-ризики).

Результатом реалізації комплаєнс-ризиків пов'язаних з конфліктом інтересів усіх названих типів, якщо вони своєчасно не ідентифікуються механізмом управління ризиками підприємства і не усуваються, можуть бути небажані наслідки. Наприклад, правового характеру (не пов'язані безпосередньо з настанням подій ризику цифровізації, викликаних з комплаєнс-ризиками): пред'явлення позовів, вимоги регулюючих органів про усунення порушень або про припинення діяльності, відкликання ліцензій, кримінальне переслідування керівників та виконавців, штрафні санкції. Всі ці наслідки впливають на фінансово-економічне становище підприємства, як у результаті виникнення безпосередніх витрат, і опосередковано у вигляді:

репутаційних витрат, втрати ділової репутації, зниження вартості бізнесу, втрати лояльності клієнтів і ринків збуту тощо;

реалізації подій технологічного ризику всіх типів: як аварійного, процесного, проектного та операційного.

Практично, безпосередня реалізація подій комплаєнс-ризиків, як правило, не обмежується для підприємства тільки безпосередньо пов'язаними з ними втратами, а й переважно супроводжується, виникненням наслідків правового і репутаційного характеру.

У процесі модернізації механізму розвитку управління ризиками та його інтеграції у загальне управління підприємства слід забезпечити реалізацію контрольно-дозвільної комплаєнс-функції наступним:

1) консультаційною підтримкою, що передбачає підтримку підрозділів підприємства у формі консультацій щодо нормативно-правового регулювання, у тому числі відстеження поточних змін регулювання та інформування про зміни;

2) постійним навчанням та підвищенням кваліфікації, що передбачає навчання персоналу щодо проблем комплаєнсу, інформуванні персоналу про поточний стан нормативно-правових документів, що регулюють їхню діяльність, роз'ясненні різних аспектів використання різноманітних регламентів, стандартів та нормативів та здійсненні діяльності в рамках існуючих бізнес-процесів;

3) формуванням комплаєнс-культури у персоналу підприємства, у тому числі, цифрового комплаєнсу − культури безпеки;

4) аналітичною підтримкою − виявлення, оцінка та аналіз поточних та потенційних комплаєнс-ризиків, зумовлених як конфліктами інтересів різного роду, так і змінами нормативно-правової та регламентної бази;

5) контролінгом − оцінка регламентів та практики бізнес-процесів (включаючи технологічні процеси) підприємства, з погляду, відповідності (комплаєнса) існуючій нормативно-правовій базі, іншим регламентам, правилам і стандартам, а також цивільно-правовим зобов'язанням підприємства [158].

Контрольно-дозвільна комплаєнс-функція підприємства може здійснюватися трьома способами:

дозвільним порядком, коли рішення виконавчих органів (накази та розпорядження, регламенти, інструкції, зміни до нормативних актів підприємства та підрозділів) щодо здійснення діяльності підприємства підлягають обов'язковому схваленню органу, відповідального за комплаєнс, як правило, вищого керівництва;

повідомчим порядком (методом моніторингу), коли інформація про прийняті рішення, здійснені дії та результати передається до підрозділу підприємства відповідального за комплаєнс. З метою проведення аналізу, видачі оцінок законності та обґрунтованості рішень і дій, вироблення рекомендацій щодо вдосконалення діяльності (при цьому визначається порядок, періодичність і склад ситуацій) вони спочатку доповідаються у

відповідні органи комплаєнсу. Наприклад, рішення про зміну технологічних та експлуатаційних параметрів (у рамках допустимих діапазонів, інформації щодо збоїв та помилок в процесах, аварійних ситуаціях тощо);

методом вибіркового спостереження – аудиту діяльності. Дана форма важлива для виявлення латентних комплаєнс-ризиків виробництва.

В механізмі розвитку управління ризиками підприємства можна виділити такі типи управлінських рішень:

стратегічні (довгострокові) рішення, коли процес розробки рішення (вираженого, як правило, у формі регламентного, нормативного документа або цивільно-правового акту (договору) займає досить тривалий час, що допускає включення етапу узгодження з відповідним підрозділом комплаєнсу, причому, прийняті рішення мають тривалий період дії (місяці, роки), до цього типу рішень слід віднести рішення щодо комплаєнс-ризиків, що відповідають конфлікту інтересів другого та третього типу: вищого менеджменту та самого підприємства щодо своїх зобов'язань.

тактичні (короткострокові) рішення, коли процес ухвалення рішення займає стислий час, рішення має виконуватися (застосовуватися) негайно, і, як правило, має обмежений час дії (конкретний цикл виробничої операції, виробнича зміна, доба), що не дозволяє, як правило, включити етап узгодження з відповідним підрозділом комплаєнсу, такі рішення відповідають за виконання оперативних виробничих завдань і відносяться до компетенції лінійного менеджменту підприємства та безпосередніх виконавців (від оператора обладнання до керівника робіт, виробничої ділянки, цеху) і співвідносяться з комплексними ризиками, зумовленими конфліктом інтересів першого типу, який характерний для рівня операційного персоналу.

Відповідно, три різних вектора дії контрольно-дозвільної комплаєнс-функція необхідні для модернізації механізму розвитку управління ризиками на різних його ієрархічних управлінських рівнях. Для стратегічних рішень управління ризиками, основним способом реалізації контрольно-дозвільної комплаєнс-функції може бути використання дозвільного порядку з використанням аудиту/вибіркового контролю (як допоміжний спосіб). При цьому використання дозвільного контролю має здійснюватися в тісному зв'язку із здійсненням консультативної підтримки.

Для тактичних рішень управління ризиками основним способом реалізації контрольно-дозвільної комплаєнс-функції є поєднання сповіщувального порядку, спільно з регулярним аудитом/вибірковим контролем. Використання дозвільного контролю, при даному типі управлінських рішень, як допоміжний тип можливе, а, в деяких випадках, функціонування технологічної системи підприємства необхідно (робота в перехідних, нестійких режимах, проведення випробувань і пусконалагоджувальних робіт, освоєння нової продукції/послуг/технологій тощо). Однак, у цьому випадку, контрольно-дозвільна комплаєнс-функція повинна делегуватися вищому рівню менеджменту, що володіє достатніми не тільки компетенціями комплаєнс-контролю, а й технічними.

Саме тому рекомендується модернізований механізм розвитку управління ризиками із запровадженням контрольно-дозвільної комплаєнс-функції та проактивних методів управління, що притаманні управлінню ризиками на підґрунті антиципації інтегрувати до процесу управління підприємством з метою поліпшення ефективності прийняття управлінських рішень, отримання ефекту постійності економічного поступу, врегулювання і збереження на високому рівні стану ризикозахищеності підприємства.

„Через те, що фундаментом механізму розвитку управління ризиками виступає стійкий, ефективно функціонуючий комплекс захисту, який базується на концепції побудови та реалізації плану ефективного застосування ресурсів підприємства, можливостей та потенціалу, протидії руйнуючій дії зовнішнього та внутрішнього середовищ, вирішальним компонентом у створенні сучасної системи управління підприємством виступає її інтеграція з системою ризик-менеджменту" [93].

Методичний підхід щодо інтеграції модернізованого механізму управління ризиками в механізм управління підприємства наведено на рисунку 3.7.

Він складається із трьох основних етапів:

Етап 1 – аудит управління ризиками, розробка відповідного плану з визначенням термінів інтеграції та необхідних для цього ресурсів.

Етап 2 − модифікації застосовуваних процесів прийняття рішень, інтеграція у ключові бізнес-процеси.

Етап 3 − забезпечення розуміння та правильного застосування механізму розвитку управління ризиками в діяльності підприємства.

Можна виділити наступні напрями інтеграції модернізованого механізму розвитку управління ризиками в загальне управління підприємства:

швидке виявлення операційних ризиків, а саме запуск процесу ідентифікації, оцінки, регулювання та моніторингу ризиків при створенні річного плану та звітності за окремими групами ризиків;

створення та реалізація програми, яка б забезпечила мінімальні операційні витрати (передусім, елементи матеріальних витрат), забезпечення результативності усіх бізнес- процесів, коригування планів в разі ліквідації форс-мажорних ситуацій;

у конкретно визначені терміни проведення аудитів бізнес-процесів підприємницької діяльності, аналіз їх ефективності та контрольованості (менеджмент має впроваджувати моніторинг на основі проведених перевірок, результати цих перевірок мають бути оголошені усім відділам та структурним підрозділам підприємства);

для мінімізації результатів ризиків потрібно активно впроваджувати страхування (на підприємстві має бути створений Департамент внутрішнього контролю, аудиту та ризик-менеджменту, який забезпечував би популяризацію ідеї страхового захисту та злагоджений зв'язок між усіма відділами та службами);

Рис. 3.7. Методичний підхід щодо інтеграції модернізованого механізму управління ризиками в механізм управління підприємства

з метою мінімізації ризиків та гарантування економічної безпеки підприємства формується і впроваджується стратегія сталого розвитку підприємства з врахуванням розроблених планів захисту від ризиків;

формування механізму управління фінансовими потоками (дасть можливість швидкого реагування у внутрішньому та зовнішньому середовищах, забезпечить високу ліквідність та платоспроможність підприємству);

побудова альтернативних сценаріїв зміни зовнішнього середовища, досягнення стратегічних цілей з урахуванням усіх можливих ризиків, регулювання різнобічних ситуацій з призначенням відповідальних осіб у кожному відділі чи підрозділі;

створення спеціального фонду так званої „фінансової подушки безпеки", що дозволить у разі настання критичної ситуації мати кошти на відновлення усіх бізнес-процесів. Особливо така форма стала актуальною при поширенні пандемії COVID-19 та воєнної ситуації в країні, оскільки жодні прогнози чи системи ризик-менеджменту не були готові до таких подій. Лише ті підприємства, які мали спеціальні фонди, змогли протриматись в умовах жорсткого локдауну, а зараз під час війни мають можливість відновлювати свою роботу або переорієнтовуватись у інші сфери діяльності [165].

Доцільно інтеграцію механізму розвитку управління ризиками у загальну систему управління підприємств, здійснювати за наступними принципами:

1. *Принцип контрольованості:* всі види діяльності повинні бути контрольованими, механізм розвитку управління ризиками має охоплювати всі функціональні підрозділи підприємства;
2. *Принцип збалансованості:* проведення економічної діагностики при прийнятті рішень щодо втрат та можливостей;
3. *Принцип комплексності:* механізм розвитку управління ризиками функціонує з єдиною базою відповідних принципів та методів з врахуванням характеру та взаємодії їх впливу, визначенням можливих наслідків подій;
4. *Принцип безперервності:* постійний моніторинг змін у внутрішньому та зовнішньому середовищі з внесенням нової інформації для механізму розвитку управління ризиками.
5. *Принцип комплаєнс-захисту:* запобігання потенційних втрат і юридичних санкцій через недотримання законів або правил ведення бізнесу.

3.2. Проактивні методи управління ризиками підприємств та нові інструменти страхування в умовах цифровізації

Незважаючи на безумовні переваги цифровізації підприємств (розвиток ІКТ, Dig Data, штучного інтелекту, технології блокчейну, хмарних обчислень, створення сучасних матеріалів, впровадження нових дифузних моделей управління), з'являються і новітні ризики, генеровані використанням новітніх цифрових технологій, що можуть негативно впливати на результати функціонування підприємств. Це зумовлює впровадження та використання

проактивних методів управління ризиками підприємств й нових інструментів страхування в умовах цифровізації.

Визначальною ознакою цифровізації підприємства вважається трансформація структури та вагомості чинників виробництва, ключовим із яких стає інформація. „Опрацювання значних обсягів даних та використання результатів їх аналізу дозволяють значно підвищити ефективність різноманітних виробництв, технологій та обладнання, зберігання, продажу і постачання товарів й послуг" [11]. Відбувається digital - трансформація бізнесу, що зумовлює використання проактивних методів управління ризиками. Поняття „проактивності" введено в науковий вжиток теорії ризиків в кінці минулого століття, фактично як протиставлення реактивності, тобто реагування на ризикові події за певних обставин. На противагу реактивним методам управління ризиками, характерними рисами проактивних слід вважати:

завчасна розробка спектру превентивних і випереджуючих заходів щодо відвернення чи мінімізації настання ризикових процесів із чітким окресленням результатів і відповідальності за ухвалення відповідних рішень;

прогнозування ризикових явищ та завчасна ідентифікація потенційних загроз і їх наслідків у стратегічному горизонті;

генерування ініціатив персоналом підприємства щодо конфігурації вибору та використання методів управління ризиками, а не реактивне пристосування до нових умов;

розробка інноваційних і креативних підходів до вибору та використання методів управління ризиками для результативного розв'язання існуючих чи нових проблем і завдань підприємства;

комплекс методів управління ризиками зорієнтований на стратегічну перспективу;

широке застосування сценарного підходу до прогнозування настання і наслідків ризикових процесів;

впровадження різноманітних цифрових комунікаційних ланцюгів та сучасних інформаційно-комунікаційних технологій.

Тобто, формування системи проактивних методів управління ризиками підприємств передбачає: ініціативність, випереджувальність, зорієнтованість, стратегічність, превентивність щодо уникнення прояву ризикових явищ і їх наслідків та максимізацію позитивних ефектів із впровадженням новаторських і креативних підходів. Фактично, проактивність передбачає вибір методів управління ризиками перед тим, як ризикові явища настануть, тобто вплив ризикових процесів прогнозується, і відповідно будується стратегія управління ризиками та розробляється спектр сценаріїв їх нівелювання чи мінімізації.

Узагальнюючи, відмітимо, що проактивні методи управління ризиками підприємств – це сукупність певних дій і заходів підприємства, які передбачають превентивне формування і використання динамічних здатностей і нових компетенцій, зорієнтований потужний вплив на

конфігурацію ризиків і загроз на підґрунті прогнозування й моделювання розвитку ризикових процесів та примноження ініціативності й креативності персоналу підприємства.

Для впровадження проактивних методів управління ризиками в підприємствах доцільно виділити спектр необхідних заходів:

своєчасне виявлення різноманітних ризиків (ідентифікація, діагностика, регулювання, моніторинг і контроль за окремими блоками ризиків і загроз);

розробка та реалізація програми щодо мінімізації витрат і забезпечення результативності усіх бізнес- процесів, коригування заходів у разі настання форс-мажорних ситуацій;

своєчасне здійснення аудитів бізнес-процесів та комунікаційних ланцюгів, аналіз їх результативності та контрольованості;

формування стратегії ризикозахищеності підприємства із конкретними планами і заходами щодо мінімізації чи нівелювання ризиків;

жорсткий контроль за фінансовими потоками підприємства;

розробка альтернативних сценаріїв розвитку ризикових процесів та виміру їх наслідків у стратегічному горизонті з урахуванням усіх потенційних ризиків та загроз;

формування „фінансової безпекової подушки", що дасть змогу забезпечити ризикозахищеність підприємства та у разі настання ризикових явищ швидко відновити необхідні бізнес-комбінації (актуальність та необхідність її формування підтвердилось процесами поширення пандемії COVID-19 та неочікуваним впровадженням воєнного часу в країні на тривалий період, оскільки жодне підприємство не було готово до них, проте підприємства, у яких вони були сформовані, змогли витримати жорсткий локдаун, а під час дії воєнного стану відновили своє функціонування, і навіть диверсифікували напрями своєї діяльності).

Для фільтрації й формування проактивних методів управління ризиків в підприємствах доцільно врахувати низку чинників: складність системи управління і організаційного дизайну підприємства, технології і якість та ефективність надання послуг чи продуктів, збалансованість розподілу управлінських функцій, складність алгоритмів бізнес-процесів, процедури взаємодії з усіма контактними аудиторіями, вимоги до компетентностей персоналу, обсяг інформаційних потоків, часові параметри для вирішення проблеми, запити партнерів та клієнтів, кількість вузлів і користувачів, стратегічні пріоритети і орієнтири підприємства, рівень цифрової зрілості підприємства, гнучкість розкладів і графіків, стабільність напрямів діяльності та команди підприємства, технологічна інфраструктура підприємства. Акцентуємо, що результативність проактивних методів управління ризиками помітно залежить від належного організаційного та інформаційного забезпечення, оскільки необхідна оперативна інформація для ухвалення відповідних заходів, а сучасний розвиток діджиталізації усіх бізнес-процесів вносить помітні зміни в обробку інформаційних потоків, водночас, важливо

враховувати рівень компетентностей управлінського персоналу щодо забезпечення бажаної результативності рішень з управління ризиками.

Доцільно використовувати оптимізацію динамічного, лінійного програмування й економіко-математичне моделювання для оцінки масштабів ризикових процесів підприємства та їх наслідків, що дасть змогу використати її при здійсненні діагностики ризикозахищеності підприємства, виявленні тенденцій розвитку ризикових подій, оцінюванні результативності методів управління ризиками та ухвалення відповідних управлінських заходів.

Крім того, система проактивних методів управління ризиками має включати:

мозковий штурм (для ідентифікації джерел загроз, ризиків та кількісної оцінки наслідків їх настання);

метод Делфі (для генерування і акумуляції експертних знань і думок щодо джерел загроз, ризиків та ефектів наслідків їх настання);

SWOT аналіз (для визначення слабких та сильних сторін кожного використання кожного методу управління ризиками);

сценарне комп'ютерне моделювання (для визначення ймовірності та масштабів настання ризикових подій, розробки різних сценаріїв розвитку ризикових процесів та виміру їх наслідків на основі методу теорії ігор, зокрема Монте-Карло);

карту ризиків (для систематизації наявних та прогнозованих загроз і ризиків та їх оцінки у розрізі бізнес-процесів та управлінських підрозділів).

Проактивність методів управління ризиками підприємства необхідна при динамізмі настання ризикових подій, складності й турбулентності економічного простору. При чому, акцентуємо, що чим більш динамічними, турбулентними, складними і невизначеними є прояви економічного простору, тим потужнішими і проактивнішими мають бути методи управління ризиками підприємства.

„Розумні" пристрої та інноваційні послуги можуть спровокувати непередбачені негативні наслідки та появу специфічних надскладних загроз (крадіжка інформації, збої комунікацій та цілих виробничих комплексів і логістичних ланцюгів). Так, за звітними даними Міжнародного економічного форуму (World Economic Forum) по глобальним ризикам, віртуальні (кібер) ризики означені, найголовнішими комерційниими ризиками. Підтверджують таке ствердження і аналітичні дані компанії Global Corporate & Specialty, які аналізували ризики щодо ведення бізнесу.

Їх дані демонструють, що кібер-ризики є найнебезпечнішими для провадження бізнесу. Так, сумарні втрати світової економіки від їх реалізації становили у 2015 році близько 445 мільярдів доларів [16, с. 10], а вже у 2017 році – 600 мільярдів доларів [18]. За аналізом Страхового брокера „ІНСАРТ" – 25 млн. дол. США – понесений збиток українським бізнесом в результаті кібер-атак, близько 50% вітчизняних компаній мали справу з кібер- атаками; більш ніж 125000 комп'ютерів було заражене внаслідок кібер-атаки вірусу Petya.A, а розмір збитків склав 466,3 млн. доларів США [18]

Більшість вчених, вважають, що кібер-ризик – це ризик, що генерується використанням: телекомунікаційного обладнання, програмного забезпечення, локальних і Інтернет-мереж, розрахунково-платіжних систем, систем інтернет-торгівлі, промислових систем менеджменту, а також це ризик, що пов'язаний з накопиченням, зберіганням, передачею і використанням персональних даних.

Змістове наповнення кібер-ризиків розкривається через їх особливості [5]:

об'єктом зазіхань (потенційної втрати) є дані (інформація) (нематеріальні активи), що несанкціоновано видаляються, спотворюються, порушується їх конфіденційність або унеможливлюється доступ до них (неавторизоване розкриття, зміна або руйнування цифрових активів);

підмножина сукупних ризиків, які відносяться одночасно до ризиків ІТ та інформаційної безпеки;

це ризики реалізації навмисних злочинних дій за допомогою використання ІТ;

результати настання кібер-ризиків можуть розглядатися з позиції видів завданих збитків (фінансовий і майновий) та суб'єктів наслідків їх реалізації (1-ша особа, 3-тя особа).

Кібер-ризики проявляються внаслідок настання таких подій:

нецільові атаки (фішинг, кардинг, sms-шахрайство);

цільові атаки (фінансове шахрайство, розкрадання баз даних, промислове шпигунство, DDoS атаки, вимагання);

атаки зсередини (розкрадання, знищення інформації, сприяння цільовій атаці).

Отже, у контексті збільшення чисельності кібер-злочинів, економічним суб'єктам необхідно розробляти шляхи їх мінімізації. Для цього використовують: технологічні рішення, просвітницьку діяльність щодо протидії кібер-злочинів, профілактичні заходи та кібер-страхування.

Кібер-страхування за ствердженням Р. Беме і Г. Шварца: це передача фінансового ризику, пов'язаного з мережевими та комп'ютерними інцидентами, третій стороні [17]. Фактично, кібер-страхування – це страховий продукт, який захищає економічні суб'єкти від ризиків, що відносяться до інформаційно-комунікаційних технологій, використання Інтернет - мережі, ІКТ-інфраструктури та діяльності у кібер-просторі.

Страховий ринок змушений адекватно реагувати на окреслені digital − трансформації і широке генерування кібер-ризиків, „задля максимального задоволення потреб і побажань своїх клієнтів з метою їх страхового захисту в частині удосконалення підходів до ведення бізнесу, розробки інноваційних каналів реалізації продуктів і надання послуг та технологій обслуговування" [9, с. 49].

Нині, рівень розвитку вітчизняного страхового ринку окреслюється: соціально-економічними реаліями в країні, готовністю економічних суб'єктів до споживання якісно нових страхових послуг, а також державною

підтримкою. „Порівняно з європейськими країнами, де страхуванням охоплено понад 94% страхового поля, в Україні страхові послуги користуються значно меншим попитом (10–15% страхового поля), особливо у галузі майнового та окремих видів особистого страхування, що зумовлено як низькою довірою економічних суб'єктів до страховиків, так і низьким рівнем їхньої обізнаності у сфері страхування" [14]. Так, за ствердженням аналітиків, „частка страхових платежів за особистим страхуванням в Україні становить усього 4-5%, тоді як у Західній Європі та США цей вид послуг займає близько 60%, у Японії – 80%, у Великобританії – 70%, а у світі в середньому – 58,3%. Загальний обсяг страхових послуг на фінансовому ринку України в останньому десятиріччі за зібраними преміями дорівнював 0,06% світового обсягу і був меншим у 400 разів порівняно із США, у 60 разів – із Німеччиною, у 50 разів – із Францією" [7, с. 413].

Останні роки спостерігається тенденція щодо зменшення кількості страхових компаній: на початок 2018 року їх кількість склала 294, з них 33 займаються страхуванням життя (СК „Life") та 261 ризиковими видами страхування (СК „non-Life") [13].

Коефіцієнт концентрації страхового ринку (CR-3) по СК „Life" сягає 54,3%, а по ризиковому страхуванню – 21,3%. У Франції цей коефіцієнт по „non-life" страхуванню становить 43,37%, по страхуванню життя – 38,54%; у Великобританії − 29,83% та 18,24%; у Нідерландах − 47,36% та 48,23% відповідно [10, с. 78]. Така висока концентрація страхового ринку України вказує на те, що вітчизняна економіка переобтяжена великою кількістю страхових компаній, частка з яких навіть не здатна надавати якісні страхові послуги, розраховуватися за власними зобов'язаннями та взагалі конкурувати за хоча б невеликий сегмент ринку [3, с. 5]. Для розвитку нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки страховий ринок варто очистити від недобросовісних страховиків та запровадити жорсткіші вимоги до показників їх ліквідності, платоспроможності, розміру мінімального капіталу, що сприятиме виконанню зобов'язань у періоди кризових деформацій.

Індекс Герфіндаля-Гіршмана (HHI) характеризує рівень конкуренції на ринку через призму його концентрації і показує розподіл „ринкової влади" між суб'єктами ринку [1, с. 302]. Для оцінки ринкової концентрації використовуються наступні діапазони даного показника: HHI<1000 − ринок оцінюється як неконцентрований; 1000< HHI<1800 – ринок оцінюється як помірно концентрований; HHI>1800 – ринок оцінюється як висококонцентрований [6, с. 83-84]. В Україні по Life-страхуванню у 2017 році цей індекс складав 1417,52 (у 2016 р. – 1079,59), а по non-Life- страхуванню, відповідно − 305,27 та 280,74. Загалом по страховому ринку індекс Герфіндаля-Гіршмана у 2017 р. становив 272,07, а у 2016 р. – 245,09.

Іншим ключовим показником вважається індекс щільності страхування. Страховий захист в країні вважається належним, якщо цей показник перебільшує 140 дол. США. Акцентуємо, що „для України характерним є

низький рівень поширеності страхових послуг, адже витрати однієї особи на страхування в середньому становлять 65,4 дол. США, в той час, як в Польщі показник щільності страхування має значення 140 дол. США, в Німеччині – 1482 дол. США, в Японії – 5-6 тис. дол. США" [21].

За таким умов, подією, що сприятиме зростанню кіберстрахування вважаємо набуття чинності регламентного документа Європейського Союзу щодо захисту даних (General Data Protection Regulation, GDPR) внаслідок підвищення обізнаності компаній про ризики, викликаних порушеннями конфіденційності при обробці даних. Регламентні нововведення надають економічним суб'єктам ЄС більше прав на свою онлайн-інформацію і передбачають штрафи обсягом до 4% річного доходу підприємств при виявленні грубих порушень. За ствердженням страхових аналітиків, цей регламент, а також широво відомі наслідки кібератак WannaCry і NotPetya сприятимуть попиту на послуги кібер-страхування. Так, кількість синдикатів Lloyd's, що пропонують кібер-страхування за 2016 рік зросла на 20%. За переконанням виконавчого директора Lloyd Інги Біль, щорічні прирости брутто-премії європейського кіберстрахування до 2020 року можуть скласти понад $ 2 млрд, що сумарно становитиме близько $ 9 млрд. Аналітики зазначають, що великі підприємства при ухваленні рішень щодо співробітництва, вимагають наявність поліса кібер-страхування у своїх контрагентів, оскільки інформаційні ресурси дорожчають, диджиталізація набирає оберти, відповідно і ймовірність фінансових і репутаційних втрат стрімко підвищується. Перспективність розвитку кібер-страхування, підтверджується і тим, що світові потужні страхові компанії вже пропонують його продукти.

Задля зростання привабливості кібер-страхування, страхові компанії розширюють страхове покриття та надають додакові послуги:

відшкодування витрат на розслідування кібер-злочинів;

антикризовий піар з метою відновлення репутації;

витрати на захист у суді і відновлення роботи ІТ-системи.

Тобто використання нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки є вигідним при великомасштабному інциденті збою чи компрометації ІКТ-системи, та сприяє економічним суб'єктам підтримувати економічну стабільність і мінімізувати втрати.

В. Братюк акцентує, що страхування кібер-ризиків спрямоване на подолання наслідків втручання кібер-злочинців (відновлення функцій, інформації, комунікацій) та пов'язане з покриттям всіх необхідних для цього витрат, а також на відшкодування збитків, які є результатом простою комп'ютерних систем [4].

Н. Приказюк вважає, що розвитку кібер-страхування заважає: невизначеність регулювання відносин у кіберстрахуванні; нестача інформації для проведення актуарних розрахунків; концентрація ризиків у разі настання страхового випадку [15]. Окрім того, відсутня необхідна статистика,

законодавча база, судова практика, недостатньо і кваліфікованих фахівців, що мають уявлення про даний вид ризику та його структуру [8].

Проведені дослідження дозволяють стверджувати, що в Україні розвиток кібер-страхування гальмується:

відсутністю фінансово потужно страхових компаній здатних прийняти кібер-ризики;

браком належної нормативної підтримки;

відсутність адекватних методик щодо ідентифікації, оцінки та систематизації кібер-ризиків;

браком достатньої статистичної та інформаційної бази для проведення актуарних розрахунків, що унеможливлює встановлення тарифів на продукти кібер-страхування;

відсутність платоспроможних страхувальників, які мають можливість придбати продукти кібер-страхування;

нормативна невизначеність статусу цифрових активів.

Нині, вітчизняні страхові компанії оцінюють кібер-ризики підприємств за допомогою непрямих ознак, показників і характеристик, серед них: наявність ризик-менеджменту, наявність служб економічної та інформаційної безпеки, способи і технології зберігання конфеденційних даних, частота проведення тестування та аудиту безпеки інформаційних потоків та комунікаційних ланцюгів, кількість IT-спеціалістів тощо.

Водночас, у цій площині, як позитив, слід відмітити диджиталізацію страхових компаній, що дозволяє їм надавати персоніфіковані послуги через зручні канали для страхувальників та ширше використання програм лояльності.

За даними Gartner „Hype cycle for property & casualty (P&C) insurance" хмарні обчислення (cloud computing) входять до п'ятірки найбільш пріоритетних IT-рішень серед страхових компаній. А, за даними Gartner, 41% страхових компаній вже використовують хмарні обчислення в своїй діяльності, ще 41% впроваджує чи планує впровадити хмарні технології в наступні 6-12 місяців. За прогнозами Gartner хмарні технології будуть широко використовуватися в страховій галузі в наступні 5-10 років [20, с.7].

25% страхувальників бажає купити страхове покриття онлайн. Нині, характерна пряма залежність між рівнем розвитку страхового ринку та часткою каналу онлайн-продажів страхових послуг серед інших каналів збуту. На розвинутих ринках частка агентського каналу складає 50-60%, на середньорозвинутих – 60-70%, на нерозвинутих – 80-90% [12].

Варто виділити наступні ключові тенденції щодо розширення каналів продажу страхових продуктів:

зростання ролі Інтернет-мережі;

широке використання різних соціальних мереж, як альтернативних каналів дистрибуції;

використання хмарних технологій, SaaS рішень тощо;

автоматизація бізнес-процесів (андерайтингу, врегулювання збитків тощо) та збільшення частки прямих продажів.

Серед ключових чинників, що сприяють нарощенню частки онлайн страхування є:

можливість обрання персоніфікованих страхових продуктів;

низька вартість страхового продукту з високою якістю;

можливість порівняння страхових продуктів страхувальниками;

зручність для споживачів.

У Великобританії понад 20% акумульованих страхових премій приходиться на онлайн-канал [2].

Водночас, слід зауважити, що вітчизняним страховим компаніям варто переймати світовий досвід для розробки пропозицій із кібер-страхування. Так, цікавим у цій площині є поліс CyberEdge від American International Group (AIG), який нині вважається вершиною розвитку кібер-страхування. Визиває інтерес, те що за даними TechCrunch, компанії Apple і Cisco уклали угоду про партнерство із страховою компанією Allianz. І тепер економічні суб'єкти, які використовують технології Apple і Cisco, мають можливість укладати більш вигідні договори з кібер-страхування з Allianz.

І сьогодні, завдяки діджиталізації страхового сегменту економічного простору генерується якісно нова сфера – InsurTech, як синтез сучасних цифрових технологій і традиційного страхування. InsurTech – це технології, які зосереджені на розробці страхових IT– рішень. До них відносять сервіси для споживачів та нові інструменти для роботи страховиків.

За інформацією IBM − 81% потужних успішних страхових компаній вже співпрацюють з InsurTech-проектами, і 45% інших страховиків. Це підтверджує тезу, що для розвитку і успішного функціонування, страховим компаніям необхідні сучасні цифрові технології.

За ствердженням McKinsey, найбільш популярними технологічними рішеннями в InsurTech-проектах є: мікрострахування (3%), блокчейн (4%), P2P (4%), робо-едвайзер (10%), гейміфікація (10%), страхування для IoT-сфери (12%), страхування на основі використання (13%), великі дані і машинне навчання (20%).

У звіті 2018 року, Edelman Trust Barometer експерти 2017 рік означують роком кризи довіри, а 2018 рік − роком битви за правду. Вірогідно, InsurTech – допоможе у цій битві.

Штучний інтелект, машинне навчання та аналіз великих даних − мають великий потенціал щодо поліпшення страхового захисту економічних суб'єктів. Big Data допоможе страховикам краще ідентифікувати й оцінити ризики. Робо-едвайзер на основі AI і machine learning допоможуть з рутинними завданнями: консультування, підбір пропозицій і рішень, оформлення необхідних документів. Нині, об'єктом страхування стає не лише майно, а й інформація. Саме це є прикметною ознакою трансформації страхового сегменту. За дослідженнями PwC, від кіберзлочинів світова економіка втрачає 400 млрд дол на рік, і цей показник буде зростати. Для порівняння (за інформацією Time з посиланням на SpaceX): запуск ракети

Falcon 9 коштує 62 млн дол, а Falcon Heavy − 90 млн дол. Вочевидь, що захищати свої бізнесові та приватні інтереси телекомунікаційні підприємства без нових інструментів та методів страхування для управління ризиками в реаліях цифрових трансформацій та без InsurTech-рішень не зможуть.

Адаптація страхового ринку до змін, пов'язаних із діджиталізацією підприємств, зміною дизайну страхових інструментів, впровадженням цифрових технологій в організацію страхової індустрії і кібер-страхування, сприятиме підвищенню якості страхового захисту й стабільному прибутковому функціонуванню телекомунікаційних підприємств, стимулюванню впровадження нових інструментів, методів, технологій і InsurTech-рішень, урізноманітненню спектру страхових продуктів, удосконаленню форм і методів страхового нагляду тощо.

3.3. Особливості розробки стратегій управління ризиками підприємств в умовах цифровізації

Сьогодні все більше керівників і менеджерів підприємств усвідомлюють необхідність змін в своєму бізнесі. Розвиток сучасних інформаційних технологій змінює способи взаємодії кінцевих споживачів з підприємствами. Сьогодні клієнт який хоче взаємодіяти з підприємством всіма доступними каналами у зручний для нього час, пов'язаний з підприємством безліччю digital-каналів: сайт, мобільні додатки, онлайн-консультанти та багато іншого. Найбільшого значення при адаптації підприємств відповідно сучасним тенденціям розвитку набуває питання їхньої цифровізації, оскільки колишні моделі і бізнес-процеси стають неефективними, старі методи комунікацій не працюють. Бурхливий розвиток інформаційних технологій, доступний Інтернет, мобільні додатки − все це змінює способи комунікації усіх контактних груп із підприємством. Багато підприємств прагнуть увійти в цифровий світ, але лише мала частина мають чіткі орієнтири для розробки стратегій управління ризиками підприємств в умовах цифровізації.

Цифровизация, діджіталізація, digital transformation, цей тренд вже міцно закріпився в програмах найбільших панельних дискусій на економічних форумах і профільних конференціях. Різні аспекти розробки стратегій управління ризиками підприємств в умовах цифровізації знаходимо у наукових розробках таких вчених: Боннет Д., Гусєва О., С., МакАфі А., Ману А., Ніл Д., Уейд М., Уестерман Г., Хаузер С.

Поняття стратегії знайшло широке відображення в багатьох наукових працях. Його родовід розпочинається з військової сфери (з грец. „стратос" − військо, „ago" − веду) де він визначався як „найважливіша складова військового мистецтва, яка опікується питаннями підготовки, планування і ведення війни, воєнних кампаній та операцій, які вирішують результат війни" [244 с. 616]. В. Даль теж тлумачив стратегію як „вчення про найкраще розміщення й використання усіх військових сил і засобів".

„Конверсія" поняття „стратегія" спостерігалась із розвитком менеджменту, у якому запозичили цей військовий термін, адаптувавши його до широкого спектру економічних умов і реалій функціонування підприємств.

Його часто трактують як план дій, що розрахований на довгостроковий період. Г. Мінцберг стверджує, що стратегія це „уніфікований, вичерпний, цілісний план... який забезпечує виконання основних завдань підприємства" [242 с. 34]. С. Єрохін, теж обгрунтовує, що стратегія − це „комплексний план, спрямований на досягнення довготермінової мети, що включає напрями, завдання та пріоритети економічного розвитку суб'єкта і комплекс відповідних заходів, дій та рішень" [237 с. 18]. Цікаво, що в теорії гри стратегія теж визначається як „складний план, план, що визначає вибір в будь-якій імовірнісній ситуації" [242 с. 34], або „множина виборів, які може бути обрано у ситуації, коли результат залежить не лише від власних дій, але й від дій інших" [255], при цьому передбачається, що стратегія формується гравцем заздалегідь та не змінюється у процесі „гри".

Дж. Б. Куїнн теж переконував, що стратегія − це „план, який інтегрує головні цілі організації, її політику та дії у певне узгоджене ціле" [242 с. 231]. А тактика, за його баченням, − це „короткострокові, адаптивні, активно-інтерактивні дії, які використовуються для досягнення цілей" [242 с. 24]. Тобто, адаптивність вважається ключовою ознакою та головною характеристикою тактики. А пріоритетне завдання стратегії зосереджено у тому, щоб окреслити контури та маркери цієї адаптивності, „вибудувати концепцію, достатньо сильну та потенційно гнучку для того, щоб організація досягла поставлених цілей наперекір усім непередбачуваним втручанням зовнішніх сил" [242 с 31]. Але, на противагу плану у якому чітко визначається перелік обов'язкових заходів та дій, стратегія має розглядатися як логіка поведінки, яка може (і повинна) модифікуватися залежно від змін зовнішнього середовища та дій конкурентів і партнерів. Г. Мольтке окреслював стратегію як „еволюцію первинної керівної ідеї у відповідності з обставинами, які постійно змінюються" [258 с. 36]. Тобто, у стратегії мають максимально враховуватися закономірності розвитку економічної системи, взаємовідносини з різними контактними аудиторіями, різноманітні бізнесові ланцюги, комунікації, коливання умов зовнішнього середовища тощо.

Таку позицію підтримує і А. Роув, обгрунтовуючи стратегічний менеджмент як „процес прийняття рішень, який об'єднує внутрішні організаційні можливості із загрозами та сприятливими можливостями, які надає зовнішнє середовище" [256]. Це, в свою чергу, потребує якнайповнішого врахування усього комплексу впливів та включення реакції на нього до програми дій. Власне, якби такі впливи були повною мірою передбачуваними, це дало б можливість звести стратегію до функціонального плану, тобто безпосередньої послідовності наперед визначених дій.

А. Чандлер визначає стратегію як „визначення основних довгострокових цілей та завдань організації, прийняття курсу дій та розміщення ресурсів, необхідне для виконання цих цілей" [248 с. 13]. З часом, еволюція розуміння

стратегії від плану до гнучкого управління за цілями прискорюється [8, с. 30]. Так, Ф. Котлер тлумачить стратегічне планування як „управлінський процес створення і підтримки стратегічної відповідності між метою і потенційними можливостями" [239 с. 538]. О. Шубін трактує стратегію як „напрямок діяльності підприємства, заснований на сполученні ресурсів і компетенції організації, що має на меті одержання конкурентних переваг на ринку" [247 с 470]. О. Гончаренко та Є. Лисицин переконують, що стратегія, „встановлює співвідношення між цілями політики і засобами їхнього досягнення" [235 с. 26]. В. Манов визначає стратегію як „генератор можливостей розвитку" [241 с. 297]. І за його переконанням, цільовою функцією стратегії є створення передумов для досягнення певних цілей. Підтримує такий підхід і Г. Почепцов, стверджуючи що „стратегія структурує майбутнє, у такий спосіб здійснюючи оптимальний перехід до нього" [243 с. 4-5].

Водночас, розглянуті підходи до поняття стратегії видаються непродуктивними у випадку, коли підприємство прагне здійснити певний цифровий прорив, освоюючи нові ринки, продукти, організаційні, виробничі чи інформаційні технології. За таких умов, невизначеність реакції зовнішнього середовища сильно зростає і унеможливлює врахування „a ргіогі" різноманітного спектру можливих дій підприємства на ці реакції. Тому й, „стратегічне планування відрізняється від звичайного врахуванням нестабільності середовища існування" [238]. Б. Будзан стверджує, що стратегія − це „набір правил, якими керуються в ухваленні управлінських рішень, щоб забезпечити здійснення місій і досягнення цілей організацій" [233 с. 71]. В. Соловуй обгрунтовує, що стратегія − це „генеральний напрямок руху, генеральна лінія поетапного досягнення мети, провідний напрямок руху для поетапного досягнення певних цілей" [245 с 66-67]. Подібне тлумачення знаходимо і у С. Мочерного: „стратегія − це довгостроковий курс економічної політики, який передбачає вирішення великомасштабних економічних і соціальних завдань" [236 с 88]. Г. Мінцберг теж окреслює стратегію за принципом „п'ять „П": план, прийоми (способи реалізації плану), поведінка, позиція стосовно інших суб'єктів та перспектива (plan, ploy, pattern of behaviour, position in respect to others, perspective) [246 с. 11]. Саме грунтуючись на такому підході, ми і будемо розглядати стратегії управління ризиками підприємств в умовах цифровізації.

Дефініція „digital" походить від латинського „digitālis" − цифри. У свою чергу поняття трансформації (transformation) − може бути розділене на „trans", тобто перетнути або змінити, а також „form", яку можна розглядати як „форму" [251]. У наукових колах ведуться жваві дискусії щодо розуміння поняття цифровізації, цифрової трансформації. Інколи їх ототожнюють із цифровим перетворенням, що передбачає „безпаперовий офіс" та досягнення „цифрової зрілості бізнесу" [253], що впливає як на окремі підприємства [249], так і на цілі сегменти економіки. Іноді цифровізацію ототожнюють із оцифровуванням (процес перетворення паперової в електронну інформацію). Але оцифрування не тотожне цифровізації чи уифровій трансформації. Тут,

важливим є комбінація стратегічних та пріоритетних взаємозв'язків, ланцюгів, дій, комунікацій які формуються для досягнення бізнес-цілей шляхом створення нових бізнес ланцюгів та оцифрування й об'єднання інформаційних масивів. Гален Груман окреслює цифрову трансформацію, як застосування цифрових технологій, що суттєво впливає на всі аспекти бізнесу та суспільства [240]. Інші дослідники визначають цифровізацію − як процес переходу підприємства до нових способів мислення і роботи на базі використання соціальних, мобільних та інших цифрових технологій. Ми підтримуємо позицію, що „цифровізація − це трансформація бізнесу шляхом перегляду бізнес-стратегії або цифрової стратегії, моделей, операцій, продуктів, маркетингового підходу, цілей тощо, шляхом прийняття цифрових технологій. Це прискорить продаж і зростання бізнесу"[257].

У багатьох випадках цифровізація передбачає кардинальну зміну організаційного дизайну, моделей та методів менеджменту, центрів відповідальності. Тобто, цифровізація це не лише використання цифрових технологій, а передусім зміни в мисленні, стилі керівництва, системі заохочення і в прийнятті нових бізнес-моделей. Водночас, акцентуємо, що цифрова трансформація передбачає інтеграцію цифрових технологій у всі сфери бізнесу, що призводить до якісних корінних змін функціонування та поведінки підприємства. По суті цифровізація − це зміна підходу до ведення бізнесу. Для того, щоб бути комерційно успішними в нових умовах загальної цифровізації, підприємству необхідно розробляти нові продукти з використанням digital-каналів підприємства. Тобто, цифрова трансформація за своїм призначенням забезпечує нові види інновацій та креативність в певній галузі, а не просто вдосконалення чи підтримку традиційних методів [254].

Нині, за оцінками експертів, більше 60% найбільших світових корпорацій вже працюють над своєю стратегією управління ризиками підприємств в умовах цифровізації.

Відповідно до індексу галузевого цифрування індексу McKinsey Global Institute [250]. Європа в даний час працює на 12% свого цифрового потенціалу, а США − на 18%. Німеччина працює на рівні 10% від свого цифрового потенціалу, тоді як Велика Британія майже порівнянна з США на рівні 17%. Це наочно демонструє, що, підприємства навіть розвинених країн, прикладаючи багато зусиль, не можуть використати весь свій потенціал цифрування.

Україна використовує менше 1% свого цифрового потенціалу. Вітчизняні підприємства не належно оцінюють такий показник, як вартість життєвого циклу закупівель і обладнання. Їх часто лякає сама перспектива IT- та цифровізації, що вимагає вкладень в оновлення інфраструктури, технологічного парку, навчання і зарплат персоналу. Водночас альтернативи цифровізації немає. Технології стрімко прогресують, набагато вищими темпами, ніж це було 30–40 років тому. Світ прискорюється, і встигнути за змінами може лише той, хто готовий вже зараз адаптуватися і перетворюватися.

Провідні світові компанії чудово усвідомлюють цей факт, про що свідчать результати недавнього дослідження „ESG 2018: Крива зрілості IT-трансформації" (ESG 2018 IT Transformation Maturity Curve), проведеного компанією Enterprise Strategy Group (ESG) за підтримки Dell EMC та Intel. Так, 96% учасників опитування, що лягло в основу цього дослідження, вже почали впроваджувати заходи з цифровізації, і вони відзначають тісний взаємозв'язок цих заходів з IT-трансформацією. При цьому 81% респондентів визнає, що без впровадження цифровізації бізнес-процесів вони були б менш конкурентоспроможними.

Звичайно, що стратегія управління ризиками підприємств в умовах цифровізації буде різнитися для кожного підприємства.

Основою цифрової трансформації мають бути технології так званої третьої платформи: хмари, мобільні сервіси, аналітика великих даних і соцмережі, що збільшує кількість каналів для комунікацій із контактними аудиторіями та переводить бізнес у on-line режим. Крім цих технологій, підприємство має перейти до нових методів імплементації проектів. Передусім, це гнучка розробка agile, яка підвищує клієнтоорієнтованість та дозволяє бізнесу і IT спільно управляти проектом ще на стадії ухвалення рішень.

Перед формуванням стратегії управління ризиками підприємств в умовах цифровізації менеджмент підприємства має з'ясувати декілька питань: чи потрібні підприємству зміни зараз; хто споживач; які точки взаємодії з клієнтами, партнерами, постачальниками; які дані про взаємодії потрібно збирати, як їх зберігати і аналізувати; яка потрібна бізнес модель для успішної діяльності; скільки підприємство може і готове інвестувати у зміни; чи готовий персонал до змін; хто буде проводити необхідні зміни.

Розробка стратегії управління ризиками підприємств в умовах цифровізації має здійснюватися за наступними етапами:

формування бачення (передусім, топ-менеджерам необхідно сформувати спільне бачення всього процесу цифровізації бізнес-процесів і донести важливість перетворень до співробітників, розробити нову систему оцінки та мотивації їх роботи);

визначення мети, цілей та завдань (необхідно розуміти, що мета успішної цифрової трансформації − це не створення нового підприємства, а його реструктуризація для того, щоб по-новому скористатися перевагами усіх наявних цінних активів і компетентностей, мають змінитися не тільки технології, але і управління та цілі і завдання, які стоять перед колективом);

проведення ретельної ревізії та аналізу стратегічних активів і компетентностей підприємства (такими активами можуть бути: кваліфікація персоналу, канали дистрибуції, продукти, партнерська мережа, дані про клієнтів тощо);

оцінка можливостей, часових обмежень, загроз та ризиків (так, часто підприємства, які роблять спробу використати можливості інтернет-маркетингу і нові бізнесові ланцюги та інформаційно-комунікаційні

технології, заходять в глухий кут через компетентнісні чи операційні дисбаланси, проблеми починаються, коли концентруються на технологіях і забувають про можливості персоналу та операційні процеси);

розробка нових схем бізнес-процесів та комунікацій (грамотна настройка усіх бізнес-процесів та комунікацій вважається надзвичайно важливим, для цього потрібно відійти від традиційної каскадної моделі поширення інформації зверху вниз і розширювати горизонтальні комунікації із використанням усіх можливих digital-каналів: електронна пошта, веб-подкасти, CRM, відеоконференції тощо);

оцінка інвестиційних можливостей, пошук мультиканального фінансування (цифровізація бізнес-процесів як будь-який процес зміни не може проходити без інвестицій, іноді їх обсяги мають бути суттєвими, а на ринку аналогічні бізнес-кейси просто відсутні, тому потрібно проводити такі зміни, які зможуть окупитися у майбутньому);

зміни у роботі з персоналом (для проведення трансформації необхідно вміти управляти новими ініціативами і процесами, для цього доводиться повністю міняти традиційні способи роботи з персоналом, деяким керівникам вдається перебудувати існуючий колектив, іншим же необхідно шукати потрібні компетенції за межами підприємства, вводяться нові посади наприклад, такі як Chief Digital Officer, Chief Data Officer, Data Scientist, директор по трансформації тощо чи створюються нові підрозділи, наприклад, Transformation Team, в яку входять фахівці з різних сфер діяльності підприємства);

своєчасне коректування стратегії (після того як дорожня карта цифрової трансформації складена і процес запущений, топ-менеджеру потрібно дуже тонко відчувати ситуацію і оцінювати зміни, що відбуваються, співробітники теж переосмислюють свою роботу, важливо бути відкритим до пропозицій персоналу, які можуть допомогти скорегувати процес перетворень і зробити його більш ефективним).

Окрім того, розробка стратегії управління ризиками підприємств в умовах цифровізації має передбачати формування кількох модулів:

клієнтський сервіс (Customer Centricity) − для підвищення клієнтоорієнтованості доцільно впроваджувати інструменти: омні-канальності, аналітики, варіативності, скоринг, адаптивності і прогнозування;

партнерство та колаборації (Partner Centricity) − розвиток інфраструктури як платформи або цілої еко-системи підприємства за принципом відкритого API і гнучкою інтеграції, що дозволить знаходити нові нестандартні проривні рішення в розвитку своїх продуктів і послуг шляхом колаборацій і інтеграцій з іншими сервісами та партнерами, цифрове партнерство стає одним з важливих чинників масштабування, що дозволяє підприємству незалежно від географії вести бізнес будь-де;

робота з даними (Data Governance) − Big Data, штучний інтелект, нейро-мережі мають стати робочими інструментами, з їх допомогою моделюється

клієнтська поведінка, прогнозується попит, формуються переваги і адаптуються продукти і послуги;

впровадження інноваційних технологій (R & D) − необхідно формувати центри інновацій (research & development), завданням яких має бути регулярна робота над пошуком і тестуванням нових напрямків розвитку бізнесу, продуктів і рішень;

цінність (Value) − використання digital дозволить підвищити цінність продуктів і послуг для клієнтів, яким стає принципово важливо купувати продукти і послуги повноцінно і дистанційно, отримувати оперативну підтримку цілодобово і без відвідування офісів, водночас змінюється економічна модель, організаційний дизайн бізнесу і модель масштабування, стають доступні нові можливості в швидкому розвитку без регіональної експансії у вигляді будівництва офісів і точок продажів;

HR-стратегія і цифрова культура інновацій (Digital culture) − у процесі перетворень підприємство переходить до клієнтоцентричної моделі, з'являється необхідність безперервного розвитку, освіти і підвищення кваліфікації усього персоналу, змінюється організаційна структура тощо.

Акцентуємо, що цифрова трансформація генерує як великі можливості, так і проблеми, перешкоди та виклики. Унікальними викликами та можливостями є те що підприємства повинні боротися гнучкими інструментами з конкурентами, які користуються перевагами низьких бар'єрів входження у бізнес, які забезпечує така технологія. Окрім того, завдяки високій важливості, наданій сьогодні технологіям та їх широкому використанню, наслідки оцифрування доходів, прибутку та можливостей мають значний потенціал зростання [20]. Основною перешкодою стає неготовність команди − відсутність розуміння і недостатність експертизи, окрім того:

на початковому етапі: брак мотивації, репутаційні ризики, відсутність перевірених бізнес-кейсів;

на етапі виконання: відсутність необхідних навичок, культурні відмінності та неефективні ІТ;

на рівні управління: не чіткість цілей, труднощі координації бізнес-процесів.

Водночас, цифровізація бізнес-процесів дає можливість заощадити, ті підприємства, які її пройшли витрачають на 31% менше на критично важливі для бізнесу додатки, та у них на 14% більше ІТ-проектів, які вони виконали, витративши менше запланованого бюджету. Можна відзначити чотири ключові переваги, які дає підприємству цифрова трансформація, згідно з даними дослідження ESG: інноваційність, прибутковість, конкурентоспроможність і економія. Шлях перетворень важко назвати легким. Однак дослідження ESG показують, що ті компанії, які вже вийшли на стадію трансформування, зуміли домогтися вагомих бізнес-результатів, зазначає віце-президент з досліджень ESG Джон МакНайт (John McKnight). За його словами, ідея ІТ-трансформації все частіше знаходить відгук у бізнесу. І вже

не тільки IT-фахівці, а й керівництво підприємств визнає її критичне і стратегічне значення.

Опитування, проведене Cisco в рамках Форуму „Інтуїтивна мережа", що відбувся у 2017 р., підтвердило важливість цифрової трансформації для вітчизняних підприємств: 38% респондентів зазначили, що спостерігають істотний вплив цього тренду на бізнес-стратегію їхніх підприємств, який триватиме протягом одного-трьох років, а 50% − вплив до певної міри. Окрім того, більше половини опитаних − 56% − стурбовані проблемами кібербезпеки, 39% − дуже стурбовані і лише 5% не переймаються ними зовсім. Показово, що за останні два роки тільки 3% респондентів не стикалися з інцидентами в галузі IT-безпеки. За цей період серед таких інцидентів частіше за інші називали віруси, поштовий спам і фішингову пошту, трояни, DDoS-атаки і програми-вимагачі. Ці атаки призводили до відмови систем (31% відповідей) та знищення даних (20%). Щодо основної перешкоди для забезпечення захисту від кіберзагроз, то тут з великим відривом серед відповідей лідирували бюджетні обмеження. На думку респондентів, вони ж посідають чільне місце в переліку перешкод на шляху digital-трансформації їх підприємств (49%). За ними йде небачення керівництвом взаємозв'язку цього тренду з бізнесом (14%), а також недостатнє розуміння того, що таке digital-трансформація і які переваги вона може принести підприємству (13%).

Таким чином, відмітимо. що стратегія управління ризиками підприємств в умовах цифровізації має передбачати здійснення перетворень у:

бізнесової діяльності: управління, маркетинг, персонал, комунікації, обслуговування клієнтів тощо.

бізнес-процесів та бізнес-ланцюгів: оптимізація та автоматизація бізнес-процесів та бізнес-ланцюгів для досягнення конкретної бізнес-цілі;

бізнес-моделі: підходи до розробки продуктів, цінової пропозиції, відношення та взаємозв'язки з клієнтами та партнерами, використання нових джерел доходів та технології, іноді зменшуючи традиційний основний бізнес;

бізнес-екосистеми: мережі партнерів та зацікавлених сторін, а також контекстні чинники, що впливають на бізнес, такі як регуляторні та економічні пріоритети та еволюція, нові екосистеми будуються між підприємствами з різним інформаційним та інноваційним фоном, завдяки яким дані та дієздатний інтелект стають інноваційними активами;

управління стратегічними активами: основна увага зосереджена на традиційних матеріальних активах, але все більше на нематеріальних активах, таких як інформація, компетенції та клієнти;

організаційний дизайн та культура: гнучкість, адаптивність, клієнтоорієнтованість, ціннісний підхід, що досягається завдяки досягненню основних компетенцій у всіх сферах, таких як цифрова зрілість, лідерство, зростання інтелектуального капіталу, креативності тощо.

Можна константувати, що, цифрова трансформація це один із найважливіших напрямів до успішного функціонування підприємства, який допоможе зробити новий бізнесовий та технологічний ривок, при цьому

істотно скоротивши витрати і оптимізуючи процеси виробництва для збереження екології. Підприємства, які сьогодні не будуть розробляти та реалізовувати свої стратегії управління ризиками підприємств в умовах цифровізації − завтра будуть неефективними і просто зникнуть під тиском нових ринкових реалій і більш прагматичних і успішних конкурентів.

Зауважимо, що з початку війни українські підприємства щодня стикаються з новими викликами та загрозами. Ризики руйнування цифрової інфраструктури, відновлювальні роботи, розмінування, міграція персоналу, зниження платоспроможності населення, інвестиційні ризики тощо – все це потребує адекватного реагування задля збереження позицій або мінімізації руйнації. Водночас, нині, як підтверджують спеціальні обстеження та наявні публікації, у більшості підприємств не сформовано стратегічних орієнтирів розвитку управління ризиками в умовах цифровізації та відсутні регламенти реагування на загрози й ризикові процеси. Водночас, як свідчать результати експертного опитування керівників та спеціалістів підприємств, переважно, керівництво та топ-менеджери підприємств добре усвідомлюють необхідність і важливість формування стратегічних орієнтирів розвитку управління ризиками в умовах цифровізації. Більше того, під час поглибленого обговорення означених питань, встановлено, що деякі керівники і спеціалісти продемонстрували обізнаність із специфікою та ключовими стратегіями розвитку управління ризиками в підприємствах. Водночас, не зважаючи на це, реальних заходів щодо системного формування і впровадження стратегічних орієнтирів розвитку управління ризиками в умовах цифровізації в практичну діяльність підприємств на підґрунті обґрунтованих теоретико-методичних засад сучасної ризикології не спостерігається.

Вагомою причиною, яка стримує процес практичного формування і впровадження стратегічних орієнтирів управління ризиками в умовах цифровізації на багатьох підприємствах, за нашими спостереженнями, вважаємо складність їх розробки та аналізу згенерованих ефектів, оскільки кількісний та якісний вимір результативності, переважно, можливий у випадку, реалізації ризикової події, а не її превенції, тому часто й нівелюються зусилля керівників й спеціалістів. Сучасна ризикологія, окреслює ризик як вірогідне явище, наслідком якого можуть бути позитивні, нейтральні або негативні ефекти.

Формування стратегічних орієнтирів вважаємо мистецтвом управління ризиками в підприємствах за умов економічних деформацій й невизначеності бізнес-процесів, що ґрунтується на прогнозуванні загроз і ризиків і використанні методів їх нівелювання чи зниження. Такі стратегічні орієнтири включають в себе регламенти, правила, стандарти, що виступають базисом для ухвалення відповідних управлінських рішень і заходів.

Метою формування стратегічних орієнтирів управління ризиками в підприємствах в умовах цифровізації є підвищення конкурентоспроможності і примноження конкурентних переваг за допомогою надійного захисту від реалізації загроз та ризикових подій.

Фактично, правилами формування стратегічних орієнтирів управління ризиками в підприємствах в умовах цифровізації слід вважати:

оптимальність поєднання прибутку і величини ризику;

максимум позитивних ефектів;

оптимальна волатильність позитивного результату;

оптимальна ймовірність позитивного результату.

Успіх формування стратегічних орієнтирів управління ризиками в підприємствах в умовах цифровізації, здебільшого, залежить від наступних чинників:

всебічна підтримка керівниками і спеціалістами;

оптимальний розподіл відповідальності і повноважень;

усвідомленість вагомості стратегічних проблем управління ризиками серед усього персоналу.

Різні управлінські ієрархічні рівні в підприємствах вимагають і різної інформаційної деталізації щодо загроз і ризиків. Так, для керівників і топ-менеджерів і головних спеціалістів ключовими завданнями мають бути:

ідентифікація та формування реєстрів ключових ризиків підприємства;

розробка ієрархічної мультимодульної карти ризиків;

розробка ризик-профіля й конкретних результативних програм в нових реаліях сьогодення;

контроль за виконанням заходів програми управління ризиками;

модернізація механізму розвитку управління ризиками;

формування гнучких організаційних структур та інформаційно-комунікаційних ланцюгів підприємства;

розробку стратегічного портфеля, корпоративної політики щодо управління ризиками;

розробка корпоративної ризик-культури персоналу;

затвердження положень, посадових інструкцій, регламентів, стандартів, форм звітності щодо управління ризиками.

Для структурних підрозділів підприємств (їх керівників і спеціалістів середньої ланки) ключовими завданнями мають бути:

ідентифікація та формування реєстрів ключових ризиків підприємства у діяльності свого структурного підрозділу;

здійснювати постійний моніторинг ефективності за виконанням заходів програми управління ризиками;

систематично надавати звіти керівництву щодо виконання заходів програми управління ризиками;

стежити за дотриманням процедур корпоративної ризик-культури персоналу.

Для кожного працівника підприємства ключовими завданнями мають бути:

у межах своїх компетенцій надавати пропозиції щодо заходів програми управління ризиками;

дотримуватись процедур корпоративної ризик-культури персоналу;

усвідомлювати важливість системи управління ризиками;

своєчасно доповідати про зміни чи відхилення щодо ідентифікації ключових ризиків підприємства.

Формування стратегічних орієнтирів управління ризиками в підприємствах в умовах цифровізації слід здійснювати за наступними етапами:

виявлення та ідентифікація ризику і діагностика ймовірності його настання та прогноз масштабу наслідків за песимістичним, оптимістичним та реалістичним сценаріями;

фільтрація та відбір методів, інструментів, технологій управління ризиками;

формування стратегічних орієнтирів, стратегічного набору та розробка відповідних ризик-стратегій задля мінімізації можливих негативних ефектів;

впровадження ризик-стратегії;

оцінка досягнутих ефектів та коригування стратегічних орієнтирів.

Ми підтримуємо наукові позиції дослідників [7], які до ключових ризик-стратегій відносять: „запобігання (уникнення), відхилення, зниження, збереження (прийняття), передача, поділ відповідальності, використання, ігнорування" [152].

Ризик-стратегії щодо уникнення ризиків в умовах цифровізації здебільшого [36, 37, 48, 89, 130] передбачають:

відмову від ненадійних постачальників, партнерів, клієнтів, тобто прагнення вести бізнес лише з надійними, перевіреними постачальниками, партнерами, клієнтами;

відмову від участі у бізнесових проектах що пов'язані із розширенням кола постачальників, партнерів, клієнтів;

відмова від інвестиційних чи інноваційних бізнес проектів ефективність яких викликає сумнів;

швидке звільнення некомпетентних спеціалістів і працівників.

Ризик-стратегії щодо збереження / прийняття ризику в умовах цифровізації здебільшого [36, 37, 48, 89, 130] передбачають:

чітке систематичне стратегічне планування бізнес діяльності, що дає змогу передбачити вузькі місця, заздалегідь ідентифікувати чинники і джерела ризиків, передбачити компенсуючі заходи чи резерви;

систематична розробка різних (песимістичного, оптимістичного та реалістичного) сценаріїв стратегічного розвитку і діагностика майбутніх викликів та запитів зовнішнього середовища;

прогнозування поведінки постачальників, партнерів, клієнтів і дій конкурентів;

моніторинг макроекономічного середовища;

формування системи резервів і запасів підприємства;

створення структурних підрозділів для імплементації ризикованих бізнес- проектів;

систематичне навчання і підвищення кваліфікації спеціалістів і працівників, розробка спеціальних інструкцій на випадок настання ризикових подій.

Ризик-стратегії щодо зниження ризику в умовах цифровізації здебільшого [36, 37, 48, 89, 130] передбачають:

зниження ймовірності настання ризикових чи несприятливих подій;

зниження обсягів можливого збитку та недоотримання бажаних обсягів прибутків,

профілактика ризиків;

диверсифікація діяльності та інвестицій;

лімітування усіх проектів та бізнес-процесів;

стратегування та хеджування ризиків;

формування матеріальних та фінансових резервів і запасів.

Ризик-стратегії щодо перерозподілу чи передачі ризику в умовах цифровізації здебільшого [36, 37, 48, 89, 130] передбачають:

пошук та залучення гарантів;

укладання договорів щодо спільної реалізації ризикованих бізнес проектів;

розподіл відповідальності між усіма учасниками бізнес-проекту;

розподіл ризику в часі (за етапами впровадження бізнес-проекту);

використання технологій аутсорсингу;

страхування ризиків.

Проте тільки зформулювати стратегічні орієнтири управління ризиками в підприємствах в умовах цифровізації недостатньо, доцільно модернізувати механізм їх впровадження, що має передбачити:

„створення ефективної системи оцінки і контролю прийнятих рішень;

виділення у структурі підприємства спеціального підрозділу (працівника), якому буде доручена організація управління ризиками;

виділення коштів і формування спеціальних резервів для реалізації механізмів управління ризиками, покриття збитків і втрат" [18, 49].

Розглянувши різноманітні підходи до формування стратегічних орієнтирів управління ризиками в підприємствах в умовах цифровізації, доцільно дотримуватись наступних положень:

„не варто ризикувати більше, ніж може дозволити власний капітал;

варто прогнозувати наслідки ризику;

не слід ризикувати багато чим заради малого;

позитивне рішення щодо обраної стратегії управління ризиками приймається лише у разі відсутності сумнівів;

у разі наявності сумнівів краще прийняти негативне рішення;

не слід вважати, що завжди існує тільки одне рішення, варто завжди порівнювати альтернативи" [42].

Цікаво, що у наукових публікаціях та світовій практиці зустрічається декілька підходів до побудови формування стратегічних орієнтирів управління ризиками в підприємствах в умовах цифровізації:

„для розвинутих країн світу характерний профілактичний підхід до стратегічних завдань управління ризиками – робота з ризиками, які ще не перетворились у проблеми;

у вітчизняних підприємствах переважно практикується реагуючий підхід – робота з ризиками, які вже стали проблемами" [139].

Для вітчизняних підприємств притаманна орієнтація на реагуючу композицію управління ризиками, водночас, потужні європейські та американські ІТ-компанії більше орієнтуються на превентивну композицію управління ризиками, тобто на новий рівень осмислення цих процесів [89, 90, 185].

Зарубіжні підприємства здійснюють безперервне формування стратегічних орієнтирів управління ризиками в умовах цифровізації, а вітчизняні підприємства характеризуються епізодичним ризик-менеджментом, тобто використовують його лише за безпосередньою вказівкою керівництва. В зарубіжних підприємствах стратегії ризик-менеджменту в умовах цифровізації координуються і коригуються керівництвом, але кожен працівник компанії розглядає стратегічні орієнтири управління ризиками як частину своїх функціональних обов'язків. На противагу цьому, кожен структурний підрозділ українських підприємств, переважно вибірково, на розсуд керівників середньої ланки намагаються управляти ризиками. В зарубіжних підприємствах уважно аналізують увесь спектр ризиків та прогнозують можливість їх реалізації, керівники вітчизняних підприємств, переважно аналізують лише ризикові події, що підлягають страхуванню чи фінансуванню.

Опираючись на основні постулати теорії стратегічного управління [36, 37, 48, 89, 130] та результати наших наукових розвідок, стратегічними орієнтирами розвитку управління ризиками в підприємствах в умовах цифровізації слід вважати наступні:

побудова ефективної системи стратегічного ризик-менеджменту на основі системного, комплексного та ситуаційного підходів;

розробка ризик-стратегій (песимістична, оптимістична та реалістична) має спиратися на науково обґрунтоване прогнозування можливих наслідків і виявлення потенційно найбільш небезпечних чинників та джерел ризиків;

розробка стратегічних та операційних планів, бюджетування;

стратегія і тактика ризик-менеджменту має затверджуватись керівництвом телекомунікаційного підприємства відповідно до мети його діяльності та його унікальних особливостей;

управління ризиками має бути неперервним комплексним процесом, координованим вищим керівництвом та впроваджуватись спільними зусиллями всього персоналу;

діагностика ринкових тенденцій і запитів потенційних клієнтів;

комплексний розгляд усього спектру ризиків з урахуванням усіх взаємозв'язків і можливих ефектів;

підвищення рівня клієнтоорієнтованості, управління взаємодій з постачальниками і партнерами;

розробка заходів програми управління ризиками;

трансформація організації бізнес-процесів, пов'язаних з технологіями та управлінням;

удосконалення організаційної структури підприємства;

покращення процедур ухвалення управлінських рішень;

забезпечення інформаційної безпеки;

підвищення кваліфікації спеціалістів та працівників;

формування корпоративної культури управління ризиками.

Регламентація реагування на загрози й ризикові процеси, відповідно до сформованих стратегічних орієнтирів в підприємствах в умовах цифровізації має передбачати:

ідентифікацію та формування реєстрів ключових ризиків підприємства;

розробку ієрархічної мультимодульної карти ризиків;

модернізацію механізму розвитку управління ризиками в підприємствах;

формування гнучких організаційних структур та інформаційно-комунікаційних ланцюгів;

затвердження положень, посадових інструкцій, регламентів, стандартів, форм звітності щодо управління ризиками;

розробку ризик-профіля й конкретних результативних програм в нових реаліях сьогодення;

розробку стратегічного портфеля, корпоративної політики щодо управління ризиками;

розробку корпоративної ризик-культури персоналу.

Формування гнучких організаційних структур та інформаційно-комунікаційних ланцюгів має передбачати надання підрозділам та посадовим особам додаткових функцій, відповідальності й повноважень щодо управління ризиками з обов'язковим передбаченням організаційної горизонтальної (між структурними підрозділами) та вертикальної (керівник – топ-менеджери – начальники підрозділів і відділів – функціональні менеджери) взаємодії щодо управління ризиками в підприємствах та має забезпечувати збір, обробку, збереження та аналіз інформаційних потоків щодо превенцій, реагування й прогнозування на загрози й ризикові процеси, підтримку ухвалення управлінських рішень, дієвість системи диспетчерського, тактичного, оперативного управління, стабільність функціонування комунікаційних ланцюгів та відповідного обладнання, систем управління активами EAM та RCM-системи тощо.

Важливим вважаємо, відповідно до сформованих стратегічних орієнтирів в підприємствах в умовах цифровізації розробку конкретних результативних програм щодо управління ризиками, модернізацію механізмів забезпечення цього процесу, впровадження постійного моніторингу й контролю за загрозами, ризиками та їх чинниками, розробку стратегічного портфеля, корпоративної політики щодо управління ризиками та корпоративної ризик-культури персоналу, формування й аналіз відповідних інформаційних баз даних тощо.

Доцільним вважаємо й визначення ефектів від сформованих стратегічних орієнтирів в підприємствах, так економічний ефект буде свідчить про підвищення прибутків, зниження собівартості продукції та послуг, організаційний ефект відображатиме якість організації процесів і процедур управління ризиками в підприємствах розширення клієнтської бази, соціальний ефект – зростання продуктивності праці, примноження компетентностей, зниження непродуктивних втрат, конфліктів, порушень трудової дисципліни, плинність кадрів тощо. Тобто використання означених стратегічних орієнтирів в підприємствах в умовах цифровізації сприятиме ухваленню більш ефективних управлінських рішень за кризових умов невизначеності, деформацій та загроз, а наявність різноманітних ефектів підтверджуватиме доцільність її практичного впровадження.

Водночас інтеграційні процеси приєднання до цифрового середовища ЄС передбачають врахування необхідності адаптації до умов конкурентного зовнішнього середовища, що зумовлює потребу врахування макро- і мезо ризиків підприємств, в основі яких має лежати розв'язання проблем довгострокового їхнього розвитку: трансформація корпоративних і конкурентних стратегій, створення цінності для всіх зацікавлених сторін, формування стратегічної поведінки, максимально відповідної умовам глобалізації та тенденціям змін цифрового світу.

Ефективність діяльності підприємств в сучасних кризових умовах повинна будуватись на основі модернізованого механізму розвитку управління ризиками. Особливо актуальне урахування ризиків і управління ними стало при необхідності переформатування всієї системи економічних відносин і життєдіяльності суспільства в наслідок пандемії COVID-19 і воєнно-політичних конфліктів. Ці зовнішні чинники внесли додаткові умови та індикативні вектори у всі бізнес-процеси і систему управління ризиками на підприємствах в умовах цифровізації, полягли в основу розробленої кватровекторної моделі розвитку управління макро- і мезо ризиками (рис. 3.8).

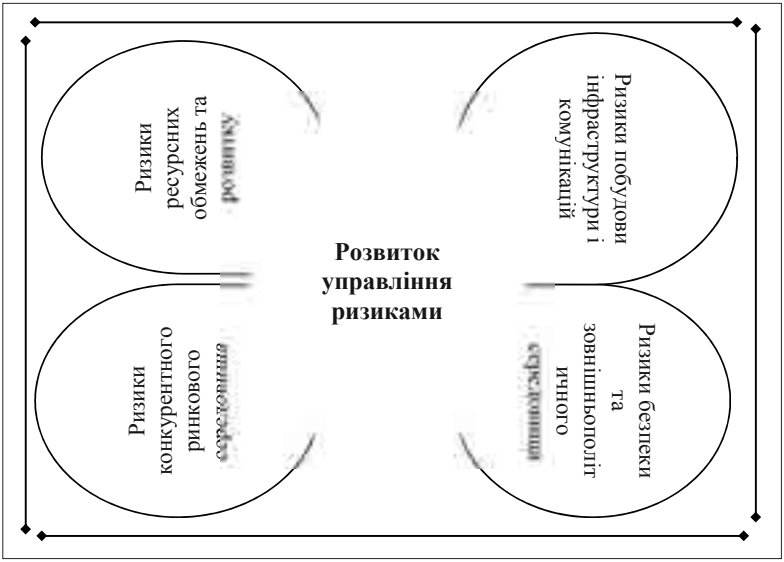


Рис. 3.8. Кватровекторна модель розвитку управління макро- і мезо ризиків на підприємствах

Примітка: сформовано з використанням *[56, 124, 125, 170]*.

Кватровекторна модель розвитку управління ризиками на підприємствах базується на чотирьох основних векторах – управління ризиками пов'язаними з ресурсними обмеженнями для забезпечення сталого розвитку; управління ризиками конкурентного ринкового середовища; управління ризиками побудови інфраструктури та комунікацій; управління ризиками з забезпечення безпеки та зовнішньополітичного оточення.

При цьому, стратегія має бути основним документом щодо розвитку управління ризиками в підприємствах в умовах цифровізації, з метою виявлення нових можливостей для отримання прибутку, забезпечення стабільного та прогнозованого перебігу подій, а значить окреслення засобів для подолання ризиків, які можуть призвести до отримання непередбачуваних збитків, або негативно вплинути на його діяльність та здатність виконувати свої зобов'язання.

Стратегія розвитку управління ризиками в підприємствах в умовах цифровізації має бути спрямованою на виявлення, визначення, оцінку та врегулювання ризиків, де оцінкою ризику є визначення його кількісних характеристик, які ґрунтуються на показниках ймовірності настання та розміру можливого збитку, а також контроль за дотриманням допустимих меж ризиків. При розробці стратегії розвитку управління ризиками в умовах цифровізації, ризики в підприємствах варто розділити на три групи: як імовірність зазнання

збитків і втрати від обраного рішення та стратегії діяльності; як імовірність відхилення від поставлених цілей; як виникнення небажаної події. Стратегія розвитку управління ризиками в умовах цифровізації є поглядом у майбутнє, плануванням, прогнозуванням і прийняттям рішень з певних дій у майбутньому. Також слід зауважити, що навіть ретельно розроблений стратегічний план матиме силу доти, поки припущення, що лежать у його основі, мають місце [170]. Д. Кент зважав на необхідність стратегічного управління ризиками та виділив стадії даного процесу [180], а А. Сливоцький виокремив сім типів стратегічних ризиків [194]. У момент формування місії та стратегічних намірів розвитку управління ризиками підприємств в умовах цифровізації мають бути окреслені ризики, що мають часові межі. Модель взаємозв'язку „стратегічні наміри-ризики", що у [170] демонструє, що прийняття рішень у площині стратегічних намірів призводить до виникнення ризиків і, навпаки, управління ризиками впливає на процес досягнення стратегічних намірів (рис. 3.9).

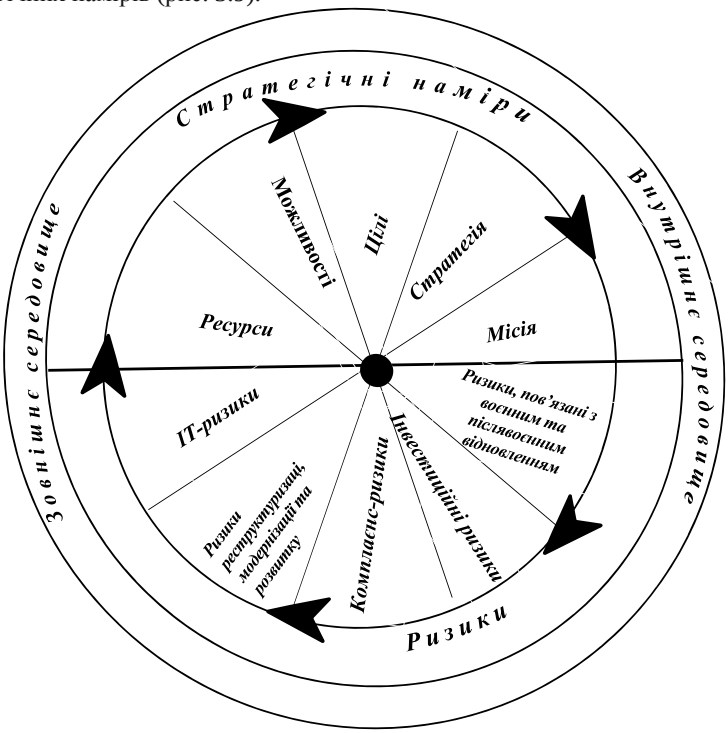


Рис. 3.9. Модель взаємозв'язку „стратегічні наміри-ризики" з уточненням ризиків стратегічного розвитку підприємств в умовах цифровізації
Примітка: побудовано за [170, 173, 178].

Розвиток управління ризиками є складовою не лише процесу формування стратегічних намірів, а й подолання негативних наслідків від будь-яких змін. Також слід зауважити, що у ході досягнення стратегічних планів відбуваються зворотний зв'язок і постійне вдосконалення сформованих стратегічних наборів. Тобто, основою для вдосконалення процесу формування стратегічних планів, на нашу думку, повинен бути розвиток управління ризиками, адже він має забезпечити передбачення несподіваних подій, формування та досягнення цілей і реалізацію стратегій у реальних умовах сьогодення, мотивування персоналу за допомогою впевненості в майбутньому підприємств, а також підвищення рівня ризикозахищеності підприємства загалом.

Аналіз виникнення можливих стратегічних ризиків в підприємствах передбачає дослідження таких основних чинників:

динаміки основних техніко-економічних показників поступу підприємств, а також підприємств суміжних галузей;

рівня конкуренції підприємств;

специфічних чинників, що характеризують функціонування та розвиток підприємств;

ринку телекомунікаційної продукції та перспектив його розвитку;

сформованої системи державного регулювання економіки та наявності державних замовлень;

показників стійкості підприємств порівняно з підприємствами суміжних галузей;

показників науково-технічного прогресу.

Доцільно виокремити блок із трьох груп завдань, вирішення яких необхідне в процесі аналізу ризиків у ході формування стратегічних планів розвитку управління ризиками підприємств:

1) група аналітико-управлінських завдань (ідентифікація та класифікація ризиків, виявлення джерел ризиків, дослідження динаміки їх взаємозв'язків і змін, визначення методів аналізу та оцінювання ризиків);

2) група виконавчих завдань (балансування послідовності дій усіх учасників процесу розробки та реалізації стратегічних намірів, контролінг дій щодо досягнення мінімального рівня ризиків сформованих стратегічних намірів, прогнозування непередбачуваних подій);

3) група координаційних завдань (застосування термінових заходів щодо коригування прийнятих стратегічних наборів і попередження наслідків наявних ризиків та виявлення методів управління ними).

Акцентуємо, що, специфікою аналізу ризиків стратегічних намірів є той факт, що за час їх розробки та реалізації можуть з'являтися нові види ризиків і змінюватися ступінь впливу вже ідентифікованих ризиків. Отже, діагностика ризиків стратегічних планів передбачає дослідження процесу розробки та реалізації цілей і стратегій спільно з аналізом усіх чинників, що визначають і впливають на запланований результат. Тому стратегічний аналіз не є дискретною дією, а розглядається як безперервний процес, що дозволяє оптимізувати ступінь впливу ризиків. З урахуванням процесу реалізації

визначеної стратегії підприємства в умовах цифровізації, доцільно проводити оцінювання рівня ризиків, які відповідають п'яти силам конкуренції за М. Портером. Так, у процесі стратегічного аналізу ризиків потрібно досліджувати учасників розробки й реалізації стратегії та ступінь їх впливу на хід реалізації плану; чинники, що впливають на процес реалізації плану, та безліч даних, що характеризують об'єкт [192 с. 218-221]. Розв'язання проблеми вимірювання ризиків підприємства в умовах цифровізації вимагає формування відповідної інформаційної бази для діагностики можливих ризиків, яка містить передусім інформацію про динаміку показників, що характеризують результати, прогнозовані в рамках стратегічних намірів, і ступінь їх чутливості до ідентифікованих ризиків. Інформація, що характеризує чинники ризику, може бути умовно розділена на такі групи: статистична інформація; облікові дані; нормативні дані; інтуїтивна інформація, заснована на досвіді та знаннях фахівців; предметний опис [192]. Для оцінювання рівня ризику можна використовувати теорію вимірювань, яка включає системний аналіз, побудову спеціальної моделі, вибір шкали вимірювання ризику і методу встановлення значень показника ризику.

Отже, концепція стратегічних орієнтирів розвитку управління ризиками сприяє результативному поступу підприємств, їх зростанню та лідерству з-поміж конкурентів у довгостроковій перспективі. Формування стратегічних орієнтирів розвитку управління ризиками в умовах цифровізації зумовлює низку переваг для підприємства, а саме: можливість поглибленого ціле встановлення для досягнення кінцевої мети існування підприємства, розроблення найменш ризикованого стратегічного набору та дієвої системи показників результативності його діяльності, підвищення ефективності управління ризиками, адаптацію до змін зовнішнього та внутрішнього середовища, підвищення гнучкості бізнес-моделі, ідентифікацію кожним працівником своєї ролі в досягненні стратегічної мети.

Контрольні питання для самодіагностики по тематиці 3 модуля

1. У чому полягає сутність розвитку управління ризиками підприємства?
2. Назвіть проактивні методи управління ризиками підприємства в умовах цифровізації.
3. Окресліть напрями активізації розвитку управління ризиками підприємств.
4. У чому полягає сутність та особливості антисипаційного управління ризиками підприємств.
5. Розкрийте поняття „стратегія управління ризиками підприємства".
6. Які розділи, зазвичай, містить стратегія управління ризиками підприємства?
7. У чому полягає основна стадія розроблення стратегії управління ризиками на підприємстві в умовах цифровізації?
8. Назвіть головні причини можливої зміни стратегії управління ризиками в умовах цифровізації.
9. Що належить до функціональних обов'язків менеджера з розробки стратегії управління ризиками на підприємстві?
10. Охарактеризуйте інноваційні інструменти страхування та методи управління ризиками підприємств в умовах цифровізації.
11. Назвіть особливості розробки стратегій управління ризиками підприємств в умовах цифровізації.
12. Перерахуйте стратегічні орієнтири управління ризиками підприємств в умовах цифровізації.
13. Аналіз виникнення можливих стратегічних ризиків в підприємствах передбачає дослідження яких основних чинників?
14. Дайте характеристику основним ризик-стратегіям підприємства в умовах цифровізації.

ПІСЛЯМОВА

Мета вивчення навчальної дисципліни „Управління ризиками підприємств в умовах цифровізації” – формування у студентів системи знань про предмет та сутність управління ризиками, його місце в діяльності підприємства, а також вироблення практичних навичок в ідентифікації, аналізі й управлінні ризиками на підприємстві в умовах цифровізації.

Предметом навчальної дисципліни є теоретичні та методичні положення щодо організації процесів управління ризиками підприємств в умовах цифровізації.

Для досягнення мети вирішено такі основні завдання:

ознайомлення здобувачів вищої освіти із теоретичними, методичними й організаційними підходами до ідентифікації та оцінювання ризиків підприємств в умовах цифровізації;

засвоєння основ організації й управління підприємствами в умовах невизначеності та ризику;

набуття теоретичних знань і практичних навичок в обґрунтуванні управлінських рішень щодо ризиків в умовах цифровізації тощо.

Професійні компетентності, яких набувають здобувачі вищої освіти після вивчення навчальної дисципліни „Управління ризиками підприємств в умовах цифровізації” можна розподілити на наступні групи:

визначення ключових аспектів виникнення ризиків у діяльності підприємств в умовах цифровізації;

виявлення джерел і природи виникнення та вияву ризиків у внутрішньому середовищі підприємства під впливом конкуренції;

виокремлення набору ризиків, згідно із класифікацією та метою аналізу;

оцінювання та прогнозування впливу ризикових ситуацій на діяльність підприємств в умовах цифровізації;

відбір та формування бази даних для оцінювання ризиків підприємств в умовах цифровізації;

оцінювання ризикових ситуацій за вибраними показниками та вимірювання розміру втрат у діяльності підприємств;

обґрунтування стратегій щодо вдосконалення та розвитку управління ризиками підприємств в умовах цифровізації;

діагностика наявної системи управління ризиками підприємств;

ідентифікація ризиків у діяльності підприємств;

визначення ефективних методів управління ризиками підприємств в умовах цифровізації;

формування стратегічних орієнтирів розвитку управління ризиками та обґрунтування напрямів зниження ступеня ризику в діяльності підприємств в умовах цифровізації.

Контрольні питання по курсу

1. Особливості функціонування підприємств за умов невизначеності.
2. Сутність та основні причини невизначеності.
3. Урахування чинника невизначеності в управлінні підприємством і засоби її зниження.
4. Характеристика критеріїв обґрунтування управлінських рішень в умовах невизначеності.
5. Сутнісно-змістова характеристика ризику.
6. Класифікація підприємницьких ризиків.
7. Детермінований еквівалент лотереї, премія за ризик та страхова сума.
8. Характеристика економічних ризиків за сферою їх походження та ступенем впливу на результати діяльності підприємств.
9. Обґрунтування управлінських рішень в умовах ризику.
10. Критерії прийняття господарських рішень за умов ризику.
11. Прийняття рішень в конфліктних ситуаціях.
12. Проектний ризик в умовах цифровізації.
13. Критерії обґрунтування рішень у процесі прийняття (вибору) проекту цифровізації.
14. Систематичний ризик та очікувана дохідність підприємства.
15. Межі застосування кількісних та якісних методів аналізу певного ризику.
16. Якісний аналіз підприємницьких ризиків.
17. Сутність системних та несистемних (унікальних) ризиків та можливості зведення їх до мінімуму.
18. Сутність політичних ризиків та їх вплив на поведінку підприємств.
19. Походження соціальних ризиків та їх співвідношення із соціальним становищем.
20. Характеристика адміністративно-нормативних ризиків.
21. Сутність податкових ризиків та їх урахування в підприємницькій діяльності.
22. Сутність інформаційних ризиків, їх класифікація та вплив на діяльність підприємства.
23. Безпосередньо ризики цифровізації, їх види та причини виникнення.
24. Сутність кіберризиків, їх види та причини виникнення.
25. Сутність цифрових ризиків, їх види та причини виникнення.
26. Характеристика ризиків у діяльності підприємства в умовах цифровізації.
27. Причини виникнення ризиків цифровізації.
28. Характеристика фінансових ризиків та їх види.
29. Сутність інвестиційних ризиків, їх види та причини виникнення.
30. Ризики зовнішньоекономічної діяльності підприємства.
31. Кількісна оцінка ризиків підприємства в умовах цифровізації.
32. Система показників абсолютного та відносного вимірювання ризику.
33. Характеристика методів кількісного оцінювання ризиків.

34. Характеристика методів оцінювання ризикованості проектів цифровізації.
35. Переваги та недоліки основних методів кількісного оцінювання підприємницьких ризиків.
36. Переваги та недоліки основних методів якісного оцінювання ризиків проектів цифровізації.
37. Особливості управління ризиками підприємства в умовах цифровізації.
38. Структурна схема механізму управління ризиками.
39. Напрями та методи регулювання ступеня ризику.
40. Методи зниження ступеня ризику.
41. Особливості механізму управління ризиками в умовах цифровізації.
42. Характеристика процесу диверсифікації, її переваги та недоліки.
43. Управління ризиками в проектах цифровізації підприємств.
44. Складові механізму управління ризиками в підприємствах.
45. Принципи побудови механізму управління ризиками в підприємствах.
46. Методичні підходи до діагностики управління ризиками підприємств.
47. Сутність і завдання ризикозахищенності підприємства в умовах цифровізації.
48. Ризикозахищенність підприємства в умовах цифровізації.
49. Сутність кіберризиків підприємства.
50. Характеристика інформаційних ризиків підприємства.
51. Управління ризиками цифровізації підприємств.
52. Напрями активізації розвитку управління ризиками підприємств.
53. Антисипаційне управління ризиками підприємств: сутність та особливості.
54. Інноваційні інструменти страхування та методи управління ризиками підприємств в умовах цифровізації.
55. Особливості розробки стратегій управління ризиками підприємств в умовах цифровізації.
56. Стратегічні орієнтири управління ризиками підприємств в умовах цифровізації.

Тестові завдання по курсу

1. Категорія ризику розкривається через наступні функції:

а) контрольна, розподільча, захисна, аналітична;

б) інноваційна, регулятивна, захисна, аналітична;

в) інноваційна, контрольна, конструктивна, аналітична.

2. Фінансові ризики відносяться до:

а) чистих ризиків;

б) спекулятивних ризиків;

в) комерційних ризиків.

3. Підприємницький ризик – це:

а) відхилення від мети, заради якої було прийнято управлінське рішення;

б) мати несподіваний збиток;

в) непевність в імовірності настання визначеного результату.

4. Ризик ліквідності – це:

а) ризик невірного вибору певного цінного папера порівняно з іншими цінними паперами при формуванні портфеля;

б) ризик утрат, що може мати банк у результаті зміни відсоткових ставок „за ризик";

в) ризик, пов'язаний з можливістю втрат від реалізації цінних паперів у результаті зміни оцінки їхньої якості.

5. Інвестор може стати банкрутом, якщо коефіцієнт ризику складає:

а) 0,1;

б) 0,3;

в) 0,5;

г) 0,9.

6. До чинників зовнішнього середовища підприємства належить:

а) рівень витрат підприємства на виробництво продукції;

б) якість продукції підприємства;

в) зв'язки з постачальниками сировини;

г) стан виробничих засобів підприємства.

7. До елементів ризику не належить:

а) суб'єкт ризику;

б) об'єкт ризику;

в) джерело ризику;

г) інформація про ступінь ризику.

8. Зовнішнім чинником ризику є такий елемент:

а) якість маркетингових досліджень;

б) схильність керівництва до ризику;

в) взаємодія з партнерами;

г) стратегія підприємства.

9. До політичних ризиків належить:

а) ризик недостатньої сегментації ринку збуту;

б) ризики непередбачуваного підвищення цін на сировину;

в) відмова нового уряду від виконання зобов'язань, узятих попереднім урядом;

г) несприятливі зміни в законодавчій базі.

10. До внутрішніх чинників ризику належать:

а) законодавство, що регулює підприємницьку діяльність;

б) стихійні лиха;

в) організація праці на підприємстві.

11. Внутрішнім чинником ризику є:

а) принципи діяльності підприємства;

б) поведінка конкурентів;

в) науково-технічний прогрес;

г) економічні зрушення у країні.

12. До комерційного ризику належить:

а) ризик націоналізації та експропріації без адекватної компенсації;

б) ризик, пов'язаний з транспортуванням товару;

в) фізичний і моральний знос основних засобів підприємства;

г) ризик військових дій та громадських заворушень.

13. До фінансового ризику належить:

а) валютний ризик;

б) ризик, пов'язаний з платоспроможністю покупця;

в) підвищення закупівельної ціни у процесі реалізації підприємницького проекту;

г) ризик розірвання контракту внаслідок дій владних структур країни.

14. До внутрішніх причин виникнення економічного ризику належить:

а) поведінка контрагентів;

б) зсуви в економічних чинниках;

в) недоліки системи управління підприємством;

г) природно-кліматичні умови.

15. До зовнішніх причин виникнення економічного ризику належить:

а) недоліки організації процесу виробництва;

б) недоліки системи управління підприємства;

в) технологічний ризик;

г) зсуви в економічних чинниках.

16. До систематичного ризику належить:

а) галузевий ризик;

б) ризик збільшення частки витрат матеріальних ресурсів;

в) ризик низького рівня дисципліни постачання;

г) ризик, пов'язаний з платоспроможністю покупця.

17. До не систематичного належить ризик:

а) фізичного та морального зносу основних виробничих засобів підприємства;

б) націоналізації та експропріації без адекватної компенсації;

в) збільшення податків та інших відрахувань внаслідок зміни ставок оподаткування;

г) військових дій та громадських заворушень.

18. До маркетингових ризиків належить:

а) ризик взаємодії з контрагентами та партнерами у процесі організації продажу продукції;

б) несприятливі зміни в законодавстві;

в) ризик збільшення ринкових цін на сировину;

г) інфляційний ризик.

19. Оцінити ступінь ризику можна шляхом розрахунку:

а) можливого збитку;

б) можливого прибутку;

в) коливання можливого результату;

г) імовірності одержання бажаного прибутку.

20. Найменший ступінь фінансового ризику має варіант вкладення капіталу з коефіцієнтом варіації, рівним:

а) 10%;

б) 15%;

в) 20%;

г) 25%.

21. Відносна оцінка ризику – це:

а) математичне очікування настання результату;

б) варіація результату;

в) коефіцієнт варіації.

22. У якому методі використовується лінія Лоренца як криву ризику:

а) аналітичному;

б) статистичному;

в) методі аналогів.

23. Найбільш розповсюдженим способом зниження фінансового ризику є:

а) диверсифікація;

б) страхування;

в) лімітування;

г) придбання додаткової інформації стосовно вибору і результатів.

24. Загальний ризик портфеля в процесі його диверсифікації:…

а) може бути зроблене елімінованим;

б) частково елімінований і може бути менше, ніж систематичний ризик;

в) не може бути менше, ніж систематичний ризик.

25. Якщо суб'єкт ринку відмовляється від хеджування, то…

а) він несе великі попередні витрати;

б) він визнає ризик;

в) він приймає на себе ризик.

26. Прибутковість фінансового активу і ризик, що асоціюється з цим активом…

а) пов'язані прямою залежністю;

б) пов'язані зворотною залежністю;

в) ніяк не пов'язані.

27. Інвестор може стати банкрутом, якщо коефіцієнт ризику складає:

а) 0,1;

б) 0,3;

в) 0,5;

г) 0,9.

28. Курсові втрати виникають…

а) у кожного підприємства;

б) у тих підприємств, що ведуть зовнішньоекономічну діяльність.

29. Якщо суб'єкт ринку відмовляється від хеджування, то…

а) він несе великі попередні витрати;

б) він визнає ризик;

в) він приймає на себе ризик.

30. Ризик пов'язаний з торговельними операціями, а також із грошовими угодами з фінансового інвестування та дивідендних платежів – це…

а) економічний;

б) операційний;

в) трансляційний;

г) прихований.

31. Інформаційний ризик підрозділяється на:

а) репутаційний та професійний;

б) ризик втрати інформації і ризик нормативного викривлення інформації;

в) нормальний та регулюючий.

32. Розрізняють наступні імовірності викривлення інформації:

а) висока, помірна, низька;

б) висока, середня, низька;

в) умовна, середня, безумовна.

33. Визначити імовірність викривлення інформації, якщо рівень внутрішнього ризику 90%, а рівень ризику суми внутрішнього контролю – 60%:

а) висока;

б) помірна;

в) низька.

34. Неспроможність підприємства задовольнити вимоги кредиторів по сплаті товарів, робіт, послуг, включаючи неспроможність забезпечити обов'язкові платежі у бюджет і внебюджетні фонди – це:

а) фінансова криза підприємства;

б) банкрутство підприємства;

в) ліквідація підприємства.

35. Зовнішньою ознакою банкрутства є:

а) скорочення попиту на ринку збуту продукції ;

б) нестабільність податкової бази ведення господарчої діяльності;

в) припинення підприємством поточних платежів за кредиторськими зобов'язаннями.

36. Існують наступні зовнішні резерви для фінансового оздоровлення підприємства:

а) диверсифікація виробництва ;

б) дефіцит власних обігових засобів ;

в) посилення міжнародної конкуренції .

37. Існують наступні внутрішні резерви для фінансового оздоровлення підприємства:

а) диверсифікація виробництва ;

б) дефіцит власних обігових засобів ;

в) посилення міжнародної конкуренції .

38. Особа, для якої пріоритетнішим є одержання гарантованого виграшу порівняно з участю в лотереї, є:

а) схильною до ризику;

б) несхильною до ризику;

в) нейтральною до ризику.

39. Схильність осіб до ризику є джерелом прибутку таких підприємств:

а) інвестиційних компаній;

б) акціонерних товариств;

в) грального бізнесу;

г) страхових компаній.

40. Для прийняття рішень в умовах ризику застосовується:

а) модель управління запасами;

б) теорія ігор;

в) моделі лінійного програмування;

г) моделі масового обслуговування.

41. Змінні витрати становлять 16 грн. на одиницю продукції. Ціна – 36 грн. за одиницю. Постійні витрати – 600 тис. грн. Точка беззбитковості дорівнює:

а) 40;

б) 60;

в) 80;

г) 400.

42. Аналіз ризику методом аналогій базується:

а) на використанні показників еластичності;

б) на інформації про наслідки раніше схвалених рішень;

в) на імітаційному моделюванні.

43. Оцінка ризику методом аналізу чутливості базується:

а) на інформації про наслідки раніше схвалених рішень;

б) на імітаційному моделюванні;

в) на використанні показників еластичності.

44. Аналіз ризику методами імітаційного моделювання базується:

а) на формуванні моделі, здатної прогнозувати значення відповідних показників ефективності об'єкта;

б) на інформації про наслідки раніше схвалених рішень;

в) на використанні показників еластичності.

45. Об'єктивний метод визначення імовірності базується:

а) на використанні оцінок ситуації керівниками підприємства;

б) на обчисленні частоти, з якою в минулому відбулась певна подія;

в) на використанні думки консультанта-експерта.

46. Аналіз ризику методами імітаційного моделювання базується:

а) на формуванні моделі, здатної прогнозувати значення відповідних показників ефективності об'єкта;

б) на інформації про наслідки раніше схвалених рішень;

в) на використанні показників еластичності.

47. Об'єктивний метод визначення імовірності базується:

а) на використанні оцінок ситуації керівниками підприємства;

б) на обчисленні частоти, з якою в минулому відбулась певна подія;

в) на використанні думки консультанта-експерта.

48. Об'єктивний метод визначення імовірності настання певної події базується:

а) на використанні суб'єктивних оцінок та критеріїв, які базуються на різних припущеннях;

б) на обчисленні частоти, з якою в минулому відбулась певна подія.

49. До внутрішніх способів оптимізації ступеня ризику належить:

а) здобуття додаткової інформації;

б) розподіл ризику;

в) зовнішнє страхування.

50. До зовнішніх способів оптимізації ступеня ризику належить:

а) лімітування;

б) розподіл ризику;

в) створення запасів, резервів;

г) диверсифікація.

51. Хеджування – це:

а) придбання цінних паперів з метою отримання прибутку від підвищення їх курсової вартості;

б) придбання біржових контрактів з метою страхування ціни на певний актив;

в) спекуляція певними активами на біржі;

г) процедура укладення біржового контракту.

Список використаної та рекомендованої літератури

1. Адамів М. Сутність та роль антисипативного управління на підприємствах. *Галицький економічний вісник*. 2010. №3 (28). С. 112-121.
2. *Активізація діяльності в менеджменті*. URL: https:// studref.com/635476/menedzhment/aktivizatsiya_deyatelnosti_menedzhmente
3. Ансофф І. Стратегічне управління. Київ. Знання. 1989. 650 с.
4. Артищук І.В. Підходи до побудови карти ризиків на основі врахування впливу базових факторів на діяльність торговельного підприємства. *Торгівля, комерція, підприємництво: збірник наукових праць*. Львів. Видавництво Львівської комерційної академії, 2011. Вип. 13, С.101-107.
5. Афанасьєв М.В., Білоконенко Г.В. *Економічна діагностика: Навчально- методичний посібник*. Харків.: ВД „Інжек", 2007. 296 с.
6. Афанасьєв Н. В., Рогожин В. Д., Рудика В.І. *Управління розвитком підприємства: монографія*. Харків. ВД „Інжек", 2003. 184 с.
7. Бакуліч О. О., Кіс І. Р., Занора В. О. Тенденції управління екологічними ризиками транспортних проєктів. *Збірник наукових праць Черкаського державного технологічного університету. Серія „Економічні науки"*. 2020. Вип. 56. С. 62–69.
8. Балла М. І. Новий англо-український словник. Понад 160 000 слів та словосполучень. 4-е вид., випр. та доп. Київ. Чумацький Шлях. 2007.668 с.
9. Баранцева С. М., Хлевицька Т. Б. Р*изикологія*: навчальний посібник. Донецьк. ДонНУЕТ, 2011. 224 с.
10. Беляєв О.О. *Механізм господарювання: сутність та форми прояву*. Київ. Вища школа, 1990. 147 с.
11. Бланк И.А. *Інвестиційний менеджмент*: навчальний посібник. Київ. Эльга: Ника-Центр, 2001. 448 с.
12. Богоніколос Н.Д. Моделі антисипативного управління у фінансовій діяльності підприємства: автореф. дис. Харків. Харк. нац. екон. ун-т. 2005. 18 с.
13. Борисова Т. Теоретичні аспекти управління ризиком на підприємстві. *Актуальні проблеми економіки*. 2005. № 7. С. 116–121.
14. Боровик М.В. *Ризик-менеджмент*: конспект лекцій. Харків: ХНУМГ ім. О.М. Бекетова, 2018. 65 с.
15. Бояринова К. О. Властивості економічної функціональності підприємства в інноваційному розвитку. *Економіка розвитку. Науковий журнал*. 2015. № 4 (76). С. 66–72.
16. Бусел В.Т. Еволюція: Великий тлумачний словник сучасної української мови Ірпінь: ВТФ Перун, 2002. 1440 с.
17. *Великий тлумачний словник сучасної української мови*. Уклад. і голов. ред. В. Т. Бусел. Ірпінь: Перун, 2007. 1736 с.
18. Вербіцька І.І. Ризик-менеджмент як сучасна система управління ризиками підприємницьких структур. *Сталий розвиток економіки*. № 5. 2013. С. 282–291.
19. Верескун М.В. Методи оцінки ефективності впровадження інформаційних систем на промислових підприємствах. *Теоретичні і практичні аспекти економіки та інтелектуальної власності*. Маріуполь, 2015. Вип. 1 (11), Т. 1. С. 21-27.
20. Виноградова О. В., Гончаренко С. В. Передумови впровадження технологій 4g і 5g як складових інноваційного розвитку телекомунікаційних підприємств України. *Економіка. Менеджмент. Бізнес*. 2016. № 4. С. 50–55.
21. Вишневська О. А. Підприємницький ризик в управлінні конкурентоспроможністю підприємств. *Економіка і суспільство*. 2016. № 7. С. 232-237.
22. Вітлінський В. В., Великоіваненко Г. І. *Кількісне оцінювання ризику у фінансово-економічній сфері*. Фінанси України. 2003. № 11. С. 16–24.
23. Вітлінський В. В., Великоіваненко Г. І. *Ризикологія в економіці та підприємництві: монографія*. Київ. КНЕУ, 2004. 480 с.

24. *Внутрішньовиробниче планування на промислових підприємствах* : навч. посіб. Свіщов М. В., Гречан А. П., Попович Л. М.та ін. Київ. Арістей, 2005. 528 с.
25. Гаркуша О.Ю. Концептуальний підхід до формування механізму управління розвитком виноробного підприємства. *Вісник Херсонського державного університету*. 2014. Вип. 6. Ч. 2. С. 128–133.
26. Гегель Г. В. Наука логіки. Київ. Наукова думка, 1997. 800 с.
27. Герасименко О.М. *Ризик-орієнтоване управління в системі економічної безпеки підприємства*: дис. … д-ра екон. наук: 21.04.02. Київ, 2021. 667с.
28. Герасимчук Н. А., Мірзоєва Т. В., Томашевська О. А. *Економічні і фінансові ризики*: навч. посібник. Київ. Компрінт, 2015. 288 с.
29. Голобородько А. Ю. Плевако Н.О. Статистичне прогнозування тенденцій розвитку телекомунікаційної сфери економіки в умовах цифровізації. *Бізнес Інформ*. 2020. №12. с. 265-270.
30. Головач Т.В., Грушевицька А.Б., Швид В.В. Ризик менеджмент: зміст і організація на підприємстві. *Вісник Хмельницького національного університету*. 2009. № 3, Т. 1. С. 157-163.
31. Горго І. О. Ризики як ключовий об'єкт управлінської діяльності сільськогосподарських підприємств. *Науковий вісник НУБіП України, Серія Економіка, аграрний менеджмент, бізнес*. 2018. № 284. С. 288-298.
32. *Господарський кодекс України*: Закон України від 16.01.2003 р. № 436-IV. Відомості Верховної Ради України. 2003. № 18–22. Ст. 144.
33. Гранатуров В. М. *Ризики підприємницької діяльності: проблеми аналізу*. Київ. Державне вид.-інф. агентство „Зв'язок", 2000. 150 с.
34. Гранатуров В. М., Литовченко І. В., Харічков С. К. *Аналіз підприємницьких ризиків: проблеми визначення, класифікації та кількісні оцінки*: монографія. Одеса. Ін-т проблем ринку та екон.-екол. досліджень НАН України, 2003. 164 с.
35. Грещак М. Г., Гребешкова О. М., Коцюба О. С. *Внутрішній економічний механізм підприємства* : навч. посіб. Київ. КНЕУ, 2001. 228 с.
36. Гришова І.Ю., Гнатьєва Т.М. Управління ризиками у контексті стратегії антикризового управління. *Український журнал прикладної економіки*. 2016. Том 1. No 3. С. 32–40.
37. Гудзь О. Є. Стратегічне управління ризикозахищенністю інноваційної діяльності підприємств. *Вісник Харківського національного аграрного університету ім. В. В. Докучаєва*. 2015. № 1. С. 3-8.
38. Гудзь О.Є. Гармонізація механізму стратегічного управління інноваційним розвитком підприємства. *Миколаївський національний університет імені В.О. Сухомлинського*. 2015. Випуск 3. С. 272-277.
39. Гудзь О.Є. Лазоренко Л.В. Ресурсне забезпечення соціально-економічного розвитку діяльності підприємств зв'язку. *Економіка. Менеджмент. Бізнес*. №1 (18), 2017. С. 5 – 10.
40. Гудзь О.Є. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. *Економіка. Менеджмент. Бізнес*. №3 (29), 2019. С. 12−19.
41. Гудзь О.Є. Старинець О.Г. Парадигма побудови системи антикризового управління підприємством. *Економіка. Менеджмент. Бізнес*. №1 (18), 2017. С. 11 – 18.
42. Гудзь О.Є., Рубцов В.С. *Управління ризиками при реалізації власних бізнесових проектів (Ризик менеджмент у малому та середньому бізнесі*): Навч. Посібник. Київ. Планета людей, 2003. 88 с. с.5 – 78.
43. Гудзь О.Є., Стецюк П.А. Концептуальні засади управління ризикозахищенністю підприємства. *Економіка АПК*. 2014. № 11. с. 61 – 68.
44. Гусєва О. Ю. *Управління стратегічними змінами: теорія і прикладні аспекти*: монографія. Донецьк. Вид-во „Ноулідж", 2014. 395 с.
45. Данчук В. Д., Козак Л. С., Данчук М. В. *Дослідження природи підприємницьких ризиків в умовах нелінійної динаміки розвитку економіки.* Вісник НТУ. 2011. Вип. 24. С. 251–265.

46. Дергачова В.В., Колешня Я.О. *Економічна безпека підприємства на засадах антикризового управління. Економіка. Менеджмент. Бізнес*. №3 (25), 2018. С. 27−35.
47. *Дергачова В.В., Манаєнко І. М. Ризикологія: управління, проекти, тренди та перспективи. Підприємництво та інновації. 2020. (11-1), с. 24-31.*
48. Дергачова В.В., Мельник В.О. Теоретичні основи формування конкурентних стратегій підприємства. *Актуальні проблеми економіки та управління*. К.: КПІ ім. Ігоря Сікорського, 2017. №11 С. 13– 18.
49. Дергачова В.В., Рудницька Ю.В. Управління ризиками зовнішньоекономічної діяльності в умовах пандемії COVID-19. *Економіка та держава*. №12, 2020. С. 15-21.
50. Державний класифікатор видів економічної діяльності, 2010. URL: https://zakon.rada.gov.ua/rada/show/vb457609-10#Text
51. Донець Л. І. *Економічні ризики та методи їх вимірювання*. Київ. Центр навч. літератури, 2006. 312 с.
52. Донець О.М., Савельєва Т.В., Урецька Ю.І. Використання міжнародних стандартів в управлінні ризиками. *Збірник наукових праць: Управління розвитком складних систем.* Київ: КНУБА, 2011. Випуск 6. С. 36-42.
53. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018 Risk Management – Principles and guidelines on implementation, IDT). URL: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
54. ДСТУ ISO Guide 73:2013. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT). Вид. офіц. Київ: Мінекономрозвитку України, 2014. 17 с. URL: https://bambangkesit.files.wordpress.com/2015/12/iso-73_2009_risk-management-vocabulary.pdf
55. ДСТУ ISO/TR 31004:2013 Управління ризиками – Керівництво з впровадження ISO 31000 (Risk management – Guidance for the implementation of ISO 31000, IDT). [Чинний від 2019-01-01]. URL: http://irpmo.com/wp-content/uploads/2018/04/ISO-31004-2013.pdf
56. Дунда С. П. Розвиток підприємства та оцінка факторів, що на нього впливають. *Ефективна економіка* № 12, 2016.
57. Дядюк М.А. Управління ризиками: кон. лекцій. Харків: Форт, 2017. 81 с.
58. *Економіко-математичне моделювання*: навчальний посібник. За ред. О.Т. Іващука. – Тернопіль: ТНЕУ „Економічна думка”, 2008. 704 с.
59. Економічна енциклопедія: у трьох томах. Т. 1. С. В. Мочерний (відп. ред.) та ін. Київ. Видавничий центр „Академія”, 2000. 864 с.
60. Євтушенко Н.О. Механізм управління конвергентно-орієнтованим розвитком телекомунікаційних підприємств. *Економіка та суспільство*. Електронне фахове видання. Мукачево: МДУ, 2017.-№11. С.220–228.
61. Єріна А.М. *Статистичне моделювання та прогнозування*. Київ : КНЕУ, 2001. 170 с.
62. Закон України „Про стимулювання розвитку цифрової економіки в Україні” від 15.07.2021 року URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text
63. Захаржевська А. А. Гусєва О.Ю. Діагностика розвитку управління ризиками телекомунікаційних підприємств. Бізнес-інформ. № 12. 2022. С. 133-140.
64. Захаржевська А. А. Управління ризиками телекомунікаційних підприємств: сутнісні аспекти. *Економіка. Менеджмент. Бізнес*. № 1-2 (39), 2022. С. 69–74.
65. Захаржевська А. А., Зеліско І. М. Глобалізаційні імперативи діагностики розвитку управління ризиками телекомунікаційних підприємств. *Управління змінами та інновації* № (4), 2022. С.9-13.
66. Захаржевська А. А., Голобородько А. Ю. Тенденції розвитку управління ризиками телекомунікаційних підприємств. *Ефективна економіка.* № (11), 2022 р. С. 1-17.
67. Захаржевська А. А., Гудзь О.Є. Проактивні методи управління ризиками в телекомунікаційних підприємствах та їх результативність. *Підприємництво і торгівля.* №(34), 2022. С.

68. Захаржевська А. А., Хаврова К.С. Система індикаторів оцінки ключових факторів впливу на розвиток управління ризиками телекомунікаційних підприємств. Бізнес-навігатор. Вип.3 (70). 2022. С. 82-86.
69. Захаржевська А. А., Євтушенко Н.О. Особливості формування механізму розвитку управління ризиками в підприємствах. *Економічний простір*. № (182), 2022 С. 61 – 66.
70. Захаржевська А. А. Аналіз розвитку управління ризиками телекомунікаційних підприємств України за основними міжнародними індексами рівня розвитку. *The 16th International scientific and practical conference "Modern science: innovations and prospects"* (December 11-13, 2022) SSPG Publish, Stockholm, Sweden. 2022. 547 p. P.453-458.
71. Захаржевська А. А. Напрями розвитку управління ризиками телекомунікаційних підприємств в нових економічних реаліях. *Актуальні проблеми управління та економічного розвитку в умовах інформатизації суспільства*: матер. наук.-практ. конф. (м. Київ, 20 грудня 2016 р.). Київ. ДУТ, ННІМП , 2016. 170 с. С. 22–23.
72. Захаржевська А. А. Принципи побудови механізму розвитку управління ризиками телекомунікаційних підприємств. *Телекомунікаційний простір XXI сторіччя: ринок, держава, бізнес*: матер. І міжнар. науково-практ. конф. (м. Київ, 18-19 грудня 2019 р.). Київ. ННІМП, ДУТ, 2019. 372 с. С. 288–290.
73. Захаржевська А. А., Гудзь О. Є. Завдання антисипаційного управління ризиками в телекомунікаційних підприємствах. *VI Міжнародна наукова конференція на тему «Від Балтики до Причорномор'я: формування сучасного економічного простору»*. Балтійський науково-дослідний інститут проблем трансформації економічного простору. Рига. Латвія. 9-10 грудня 2022 р.
74. Захаржевська А. А., Гудзь О. Є. Методи управління ризиками в телекомунікаційних підприємствах на проактивній основі. *Актуальні проблеми економіки, фінансів, менеджменту і права: збірник тез доповідей міжнародної науково-практичної конференції* (Житомир, 2 грудня 2022 р.): у 2 ч. Житомир: ЦФЕНД, 2022. Ч. 2. 59 с. С.45-46.
75. Захаржевська А. А. Результативність управління ризиками телекомунікаційних підприємств. *Сучасні тенденції та перспективи розвитку системи управління в Україні та світі*: матер. міжнар. науково-практ. конф. (м. Київ, 16-17.03. 2017). Київ. ДУТ, 2017. 257 с. С. 29–30.
76. Захаржевська А. А. Сутнісні характеристики управління ризиками телекомунікаційних підприємств. The 8th International scientific and practical conference *„Modern research in world science"* (October 29-31, 2022) SPC "Sci-conf.com.ua", Lviv, Ukraine. 2022. 1828 p. P.1300-1304.
77. Захаржевська А. А. Концепція удосконалення управління ризиками телекомунікаційних підприємств на антиципаційній основі. *Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку*. Матер. міжнар. науково-практ. конф. (м. Київ, 11.02.2020). Київ. ННІМП, ДУТ. 2020. 250 с. С. 94–97.
78. Захаржевська А. А. Управління ризиками в умовах цифрової трансформації телекомунікаційних підприємств в постковідний період. Міжнародна конференція для країн Європи *„Цифрова трансформація як стратегічний напрям розвитку цифрової економіки в світі та в Україні"* (м. Київ, Україна) 28 грудня 2022 р. С. 17-19.
79. *Звіт „Про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації" за 2021 рік*. URL: https://nkrzi.gov.ua
80. *Звіт. „Швидка оцінка завданої шкоди та потреб на відновлення України"*. Серпень 2022. Світовий Банк, Уряд України, Європейська Комісія. URL: https://www.kmu.gov.ua/news/uriad-ukrainy-ievropeiska-komisiia-ta-svitovyi-bank-prezentuvaly-zvit-shvydka-otsinka-zavdanoi-shkody-ta-potreb-na-vidnovlennia
81. Зеліско І. М., Сосновська О. О. Аналіз впливу глобальних ризиків сучасності на функціонування вітчизняних підприємств зв'язку. *Бізнес Інформ*: науковий журнал. Харків: Інжек, 2018. № 12. С. 232–238.

82. Зінченко О. А., Зінченко Д. С. Теоретико-методичні аспекти удосконалення функціонального управління інноваційним розвитком промислових підприємств. *Підприємництво та інновації*. 2018. № 5. С. 26–33.
83. Івахненков С.В. *Інформаційні технології в організації бухгалтерського обліку та аудиту*: навч. посіб. Київ. Знання, 2006. 350 с.
84. Івченко І.Ю. *Економічні ризики*: навчальний посібник. Київ: „Центр навчальної літератури". 2004. 304 с.
85. Каміньська Б. Аналіз потенціалу розвитку промислового підприємства в антисипативному управлінні. Економічний вісник ЗДІА. 2018. № 4(16), с. 82-87.
86. Караєва Н.В., Войтко С.В., Сорокіна Л.В. *Ризик-менеджмент сталого розвитку енергетики: інформаційна підтримка прийняття рішень*: навчальний посібник. Київ: Альфа Реклама, 2013. 308с.
87. Кіберполіція: рівень уразливості майже половини інформаційних систем приватного та державного секторів критичний. *Дебет-Кредит*. 2017. URL: https://news.dtkt.ua/state/other/44693
88. Князєва О А., Шамін М.В. Формування кадрового резерву для забезпечення розвитку інтелектуального потенціалу персоналу підприємства. *Соціально-економічні проблеми сучасного періоду України*. Львів, 2019. № 5 (139). С. 49-55.
89. Князєва О.А. Стратегічні вектори економічного розвитку країни у післявоєнний час. *Науковий вісник ОНЕУ*. № 3-4 (292-293), 2022. С. 94-100.
90. Князєва О.А. Стратегія забезпечення конкурентних переваг малих та середніх телекомунікаційних підприємств. *Економіка. Менеджмент. Бізнес*. № 1(27). Київ, ДУТ. 2019. С. 4-11.
91. Ковальова Т.В., Євтушенко Н. О. *Економічний ризик: оцінка, прогнозування та шляхи мінімізації на промислових підприємствах*: монографія. Харків: ХНАДУ, 2013. 180 с.
92. *Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки*. URL: http://zakon.rada.gov.ua/laws/show/67–2018–%D1%80 .
93. Кутергина Г.В Аналіз ефективності систем управління фінансовими ризиками комерційного підприємства. *Аудит і фінансовий аналіз*. 2010. № 3. С. 149-162.
94. Кутковецький В.Я. *Ймовірнісні процеси і математична статистика в автоматизованих системах*. Миколаїв: МДГУ ім. Петра Могили. 2003. 168 с.
95. Легомінова С. В. *Теоретичні та методологічні аспекти управління конкурентними перевагами телекомунікаційних підприємств*: монографія. Київ. Міленіум, 2018. 380 с.
96. Ліпич Л., Глубіцька Т. Парадигма антисипативного управління еколого-економічних систем підприємства. *Економічний часопис Східноєвропейського національного університету імені Лесі Українки*. 2015. № 4. С. 46-53.
97. *Літовченко І. В. Обґрунтування складу ризиків та їх рівня при оцінці загроз діяльності підприємства: дис. … канд. екон. наук: 08.01.06 – „Економіка, організація і управління підприємствами" ОНАЗ ім. О. С. Попова. Одеса, 2003. 170 с.*
98. *Лозовський О. М. Основні методи оцінки рівня ризиків у процесі управління підприємством. Молодий вчений. 2014. № 5(1). С. 138-141.*
99. *Лоскоріх Г.Л. Облікове відображення зниження ризику діяльності ІТ-підприємств. Інфраструктура ринку. 2021. № 58. С. 105-108.*
100. Лук'янова В. В. *Економічний ризик*: навч. посіб. Київ. Академвидав, 2007. 262 с.
101. *Лук'янова В.В. Діагностика функціонування економічних систем з урахуванням фактору ризику. Вісник соціально-економічних досліджень. 2012. № 121 (44). С. 239-245.*
102. *Луців О. Стратегічний аналіз оптимальної поведінки підприємства в умовах невизначеності. URL:* http://www.irbis–nbuv.gov.ua
103. *Ляшенко В. І. Регулювання розвитку економічних систем: теорія, режими, інститути: монографія. Донецк: ДонНТУ, 2006. 668 с.*

104. Мала Н. Т. Економічний розвиток підприємства: планування та моделювання. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку. Вісник Національного університету Львівська політехніка*. 2012. Випуск №739. С. 22–28.
105. Матвієнко-Біляєва Г. Л. Ризик-менеджмент як сучасна система ефективного управління ризиками підприємницьких структур. *Молодий вчений*. 2018. No4. URL: http://www.donnuet .edu.ua/ index. php/en/nauka/holoshennia/1413-zbirka-tez-za-robotoiu-e
106. Мельник О. Г. Адамів М. Є. Антисипативне управління підприємствами на засадах слабких сигналів. *Актуальні проблеми економіки*. 2013. № 1. С. 32-41.
107. Месюра В. І., Ваховська Л. М., Колодний В. В. *Системи прийняття рішень з нечіткою логікою*. Частина 1. Математичні основи нечіткої логіки. Вінниця : ВНТУ, 2014. 124 с.
108. *Методи стимулювання і мотивації навчальної діяльності. Менеджмент*. URL: https://intellect.icu/aktivizatsiya-i-stimulirovanie-6641
109. Миколайчук І.П. Формування організаційно-економічного механізму управління ризикозахищеністю підприємства. *Академічний огляд*. 2018. № 2 (49). С. 45-51.
110. Мирошниченко Г. О. Управління ризиками підприємницьких структур: аспекти ризик-менеджменту. *Економіка та суспільство*. 2022. № 44. С. 87-93.
111. Мізюк Б.М. Фінансовий механізм управління ризиками підприємств. *Фінанси України*. 2003. № 11. С. 66-67.
112. Мороз В.М. Мороз С.А. *Ризик-менеджмент*. Харків: НТУ «ХПІ», 2018. 140 с.
113. Надтока Т. Б. Соціальний розвиток промислового підприємства та механізми його управління. *Управлінські технології у рішенні сучасних проблем розвитку соціально-економічних систем*: монографія. За заг. ред. О. В. Мартякової. Донецьк: Вид-во ДонНТУ, 2011. 744 с. С. 564-569
114. Нікіфоров М.М. Особливості управління ризиками телекомунікаційних підприємств. *Держава та регіони. Серія: Економіка та підприємництво*, 2020, № 6 (117). С. 67-69. URL: http://www.econom. stateandregions.zp.ua/journal/2020/6_2020/12.pdf
115. Новак Н. Г., Гаценко С. В. Організаційно-економічний механізм розвитку виробничого підприємства у змінному середовищі. *Економіка. Менеджмент. Бізнес*. 2014. № 3. С.117–123.
116. Новосад В. П., Селіверстов Р. Г. *Методологія експертного оцінювання*: конспект лекцій. Київ. НАДУ, 2008. 48 с.
117. *Огляд цифрової трансформації економіки України в умовах війни (жовтень 2022)*. URL: https://niss.gov.ua/news/komentari-ekspertiv/ohlyad-tsyfrovoyi-transformatsiyi-ekonomiky-ukrayiny-v-umovakh-viyny
118. *Офіційний сайт Державної служби статистики України*. URL: www.ukrstat.gov.ua
119. Офіційна інтернет сторінка *The Committee of Sponsoring Organizations of the Treadway Commission* (COSO). URL: https://www.coso.org/Pages/guidance.aspx.
120. *Офіційний сайт Міжнародної організації зі стандартизації* (International Organization for Standardization, ISO). URL: https://www.iso.org/committee/629121/x/catalogue/
121. *Офіційний сайт Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації*. URL: https://nkrzi.gov.ua
122. *Офіційний сайт ПАТ „Укртелеком*". URL: http://www.ukrtelecom.ua.
123. *Офіційний сайт ПрАТ „Київстар"*. URL: http://www.kyivstar.ua.
124. Підкамінний І. М. Системні фактори впливу на інноваційний розвиток підприємства. *Ефективна економіка*. 2011 рік. Випуск № 3. URL: http://nbuv.gov.ua/UJRN/efek_2011_3_4
125. Плугіна Ю. А. Інтелектуальний розвиток: сутність поняття. *Вісник економіки транспорту і промисловості*. Харків. 2011 рік. Випуск № 36. С. 193-195.
126. Побережний Р. О. Сутність стратегій розвитку підприємства: класифікаційний аспект. *Економічний вісник ЗДІА*. 2016. Вип. 5(1). С. 129-135.
127. Погорелов Ю. С. *Оцінювання та моделювання розвитку підприємства*: монографія. Луганськ. Глобус, 2010. 512 с

128. Погорєлов Ю. С. Категорія розвитку та її експлейнарний базис. *Теоретичні та прикладні питання економіки.* 2012. Вип. 27(1). С. 30–34.
129. Полінкевич О. М. Адаптивний механізм управління змінами у бізнес-структурах в умовах covid-19. *European scientific journal of Economic and Financial innovation.* 2020. №2(6). С. 173-182.
130. Пономаренко В. С., Тридід О. М., Кизим М. О. *Стратегія розвитку підприємства в умовах кризи*: монографія. Харків. ВД „ІНЖЕК", 2003. 328 с.
131. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або запобігання тероризму: Закон України від 28.11.2002, № 249-IV. *Верховна Рада України: Офіційний сайт*. URL: http://zakon4.rada.gov.ua/laws/show/249-15.
132. Про затвердження Методики виявлення ризиків, пов'язаних з державно-приватним партнерством, їх оцінки та визначення форми управління ними: Закон України від 16.02.2011 р. №232. *Верховна Рада України: Офіційний сайт*. URL: http://zakon3.rada.gov.ua/laws/show/232-2011-%D0%BF
133. Про затвердження Методичних рекомендацій щодо організації проведення перевірок підприємств, які входять до складу фінансово-промислових груп, інших об'єднань та великих платників податків: Закон України від 16.07.2007р. №432. *Державна фіскальна служба України: Офіційний портал*. URL: http://sfs.gov.ua/yuridichnim-osobam/podatkoviy-kontrol/nakazi/print-66306.html
134. Про затвердження термінологічної бази системи внутрішнього контролю та аудиту Державного казначейства України": Закон України від 07.10.2008 р. №417. *Законодавство України: Платформа ligazakon.* URL: http://search.ligazakon.ua/l_doc2.nsf/link1/DKU0702.html
135. Про об'єкти підвищеної небезпеки: Закон України від 18.01.2001, № 2245-III. *Верховна Рада України: Офіційний сайт*. URL: http://zakon0.rada.gov.ua/laws/show/2245-14
136. Проект Положення про організацію системи управління ризиками в надавачах фінансових послуг та небанківських фінансових групах. URL: https://bank.gov.ua/admin_uploads/article/proekt_Regulation_SUR_2022-06-27.pdf.
137. Прохорова В. В. Антикризове управління підприємством як система заходів його ефективного розвитку. *Вісник Національного технічного університету «Харківський політехнічний інститут». Збірник наукових праць. Тематичний випуск: Технічний прогрес і ефективність виробництва*. Харків: НТУ «ХПІ». 2009. № 35. С. 12-21.
138. Раєвнєва О. В. *Управління розвитком підприємства*: методологія, механізми, моделі : монографія. Харків: ВД «ІНЖЕК», 2006. 496 с.
139. *Ризикогенність та страхування в аграрній сфері (теорія, практика):* колект. монографія/ за заг. ред. д.е.н., проф. Є. І. Ходаківського. Житомир: Полісся, 2013. 323 с.
140. Ріщук Л.І. Формування програми ризик-менеджменту для нафтопереробного підприємства. Економіка і суспільство. 2016. № 2. С. 351 – 357.
141. Рубанов М. М. Система раннього попередження загроз за слабкими сигналами. *Вісник ХНУ. Економічні науки*. 2013. № 3(2). С. 257-261.
142. Руденський Р.А. Моделювання процесів антисипативного управління економічною безпекою: автореф. дис. на здобуття наук. ступеня канд. екон.наук: спец. 08.03.02 Економіко-математичне моделювання. Донецький нац. ун-т. Донецьк. 2002. 16 с.
143. Савченко Ю. В., Солоненко М. В. Управління ризиками на підприємствах сімейного бізнесу. *Економіка і організація управління*. 2019. № 2 (34). С. 28-36.
144. Свідерська А. В. *Управління ризиками зовнішньоекономічної діяльності підприємства:* Дис. ... канд. екон. наук: 08.00.04. Хмельницький: ХНУ, 2016. 290 с.
145. Секерін В., Мазур І. Методичні аспекти оцінки масштабів тіньової економіки. *Економіка України*. 2004. № 8. С. 36-44.
146. *Семенова К., Тарасова К. Ризики діяльності промислових підприємств: інтегральне оцінювання: монографія. Одеса: Гуляєва В.М., 2017. 234 с.*

147. *Система ризик-менеджменту в банках: теоретичні та методологічні аспекти: монографія. За ред. В. В. Коваленко. Одеса: ОНЕУ, 2017. 304 с.*
148. *Словник української мови*: в 11 т. Київ. Наукова думка. 1973. Т 4. С. 275.
149. Сосновська О. О., Деденко Л. В. Ризик-менеджмент як інструмент забезпечення стійкого функціонування підприємства в умовах невизначеності. *Європейський науковий журнал Економічних та Фінансових інновацій*. 2019. № 1(3). С. 70–79.
150. Сосновська О.О. Система економічної безпеки підприємств зв'язку: монографія. Київ. „Центр учбової літератури", 2019. 440 с.
151. Старостіна А. О. Кравченко В. А. *Ризик-менеджмент: теорія та практика*: навчальний посібник. Київ. ІВЦ „Політехніка", 2014. 200 с.
152. *Стратегічні напрями соціально-економічного розвитку аграрного сектору економіки України*: колективна монографія. За заг. редакцією А. В. Руснак. Херсон. ТОВ „ВКФ СТАР ЛТД", 2017. 432 с.
153. Стрельбіцька Н. Уніфікований міжнародний стандарт ризик-менеджменту як відповідь на виклики глобалізації. *Соціально-економічні проблеми і держава*. 2011. Вип. 2 (5). URL: http:// sepd.tntu.edu.ua /images/stories/pdf/2011/11snynvh.pdf
154. Супрун А.А. Ризики в діяльності підприємств гірничо-металургійного комплексу: види, методи, оцінки та фінансування. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління*. Том 31 (70). № 3, 2020. С. 95 – 102.
155. Тарасова Г.О. Забезпечення планування роботи з сигналами в антисипативному управлінні розвитком промислового підприємства. Економіка та суспільство. 2018. № 18, с. 72-77.
156. Тарашевський М. М. Стан управління ризиками на транспортних підприємствах України. *Бізнес-інформ. Економіка транспорту та зв'язку*. 2020. № 8. С. 125-133.
157. Тітова С. П. Особливості прояву ризику в діяльності сільськогосподарських підприємств. *Економіка АПК*. 2009. № 14. С. 33–36.
158. Українські компанії почали впроваджувати комплаєнс-контроль. Що це і навіщо? URL: https://youcontrol.com.ua/articles/komplaiens-kontrol-shcho-tse-i-navishcho/
159. *Управління підприємницьким ризиком*. За заг. ред. Д.А. Штефанича. Тернопіль. Економічна думка, 1999. 224 с.
160. Устенко О. Л. *Підприємницькі ризики: основи теорії, методологія оцінки та управління*. Київ. Всесвіт, 1996. 146 с.
161. Устенко О. *Теорія економічного ризику*: монографія. Київ. МАУП, 1997. 164 с.
162. Фролова Л.В. *Механізми логістичного управління торговельним підприємством* : монографія. Донецьк: ДонДУЕТ ім. М. Туган-Барановського, 2005. 322.
163. *Халімон Т. М. Механізм управління конкурентоспроможністю телекомунікаційних підприємств. Інтелект XXI. 2016. № 5. С. 127–131.*
164. *Цвігун Т.В. Механізм управління ризиками в системі управління підприємством. Науковий вісник Міжнародного гуманітарного університету. 2014. С. 9−13.*
165. Чайкіна А.О., Золотар К.В. Основи формування системи ризик-менеджменту на підприємстві. *Економічний розвиток держави та її соціальна стабільність*: матеріали Міжнародної науково-практичної Інтернет- конференції, 14 червня 2021 р. Полтава : Національний університет імені Юрія Кондратюка, 2021. С. 47-48.
166. Черненко Ю. О. Вибір методів управління ризиками на промисловому підприємстві. *Вісник ОНУ. Серія : Економіка*. 2014. Т. 19, Вип. 1(2). С. 36-39.
167. Чечетова Н. Ф. Ризики, їх природа, класифікація і способи виміру на ринку цінних паперів. *Зб. наук, праць ЧДТУ. Серія: Економічні науки*. 2018. Вип. 22. С. 123-126.
168. Шандова Н. В. Рушійні сили стійкого розвитку промислового підприємства. *Економічні інновації*. 2013 рік. Випуск №54. С. 354–362.
169. Швець Ю. О. Ризики в діяльності промислових підприємств: види, методи оцінки та заходи подолання ризику. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні ек. відносини та світове господарство*. 2018. Вип. 17(2). С. 131-135.

170. Швиданенко Г. О., Бойченко К. С. *Розвиток підприємства: стратегічні наміри, ризики та ефективність*: монографія. Київ. КНЕУ, 2015. 231 с.
171. Шегда, А.В. *Ризики в підприємництві: оцінювання та управління*: навч. посіб. Київ. Знання, 2008. 271 с.
172. Шпакова Г. В. *Детермінація системи оцінки еколого-економічних ефектів на основі індикаторів біосферосумісного виробництва*. URL: http://www.economy.nayka.com.ua/pdf/3_2020/79.pdf
173. *Що таке комплаєнс-ризики та як ними управляти*. URL: https://bakertilly.ua/news/id44586
174. *2021 Global ICT Development Index* – ITU. URL: https://www.itu.int/net4/ITU-D/idi/2017/index.html
175. *A Risk Management Standard. The Institute of Risk Management*: 2002. URL: https://www.theirm.org/media/6827/arms_2002_irm.pdf
176. Activation. *BCMpedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR).* URL: https://www.bcmpedia.org/wiki/Activation
177. *Aric Wood. What is "Strategy Activation*"? February 23, 2022. URL: https://xplane.com/what-is-strategy-activation/
178. BDO's *2021Telecommunications Risk Factor Survey. Risks in the new reality facing telecom companies*
179. *Brand Activation Management and your business: how to take control of your brand.* 26 May 2022. URL: https://www.papirfly.com/blog/brand-activation-management/brand-activation-management-and-your-business-how-to-take-control-of-your-brand/
180. Davis J. Sherman Kent's final thoughts on analysis Bpolicymaker relations . *The Sherman Kent Center for Intelligence Analysis*. Occasional Papers, 2003. Vol. 2. No 3. Pp. 43–44.
181. Dergachova V., M. Kravchenko, O. Vynogradova, K. Kuznietsova, V. Holiuk. Determinant management of competitive devaluation: theoretical and practical aspects. *Financial and credit activities: problems of theory and practice.* No 1 (36). 2021. №1. pp. 281-292.
182. *Enterprise Risk Managament – Integrating with Strategy and Perfomance.* URL: https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf
183. *Global Open Data Index*. URL: https://index.okfn.org/ place/? fbclid= IwA R1jXf7Wo_ XqfwW8TT6f2XT9QP5- o0umpV2HSm CsJ3nuZgeYQjkOz_a2Cbo
184. Gudz O., Prokopenko N. , Korsakov D., Solovei N. Insurance And Innovative Technologies Of Risks Management Of Ukrainian Companies In The Digital Economy. *Estudios de Economia Aplicada* 2020. Vol. 38, No 3 (1). URL: http:ojs.ual.esojsindex.phpeea.
185. Jankelova N., Masar D., Moricova S. Risk factors in the agriculture sector. *Agric. Econ. Czech.* 2017. 63:247-258.
186. Kaplan R. S., Norton D. P. *Using the Balanced Scorecard as a Strategic. Management System.* Harvard. Business Review, 1996, 325 p.
187. Kathie Fuce-Hobohm. *What is Activation*? URL: https://spaceinc.net/what-is-activation/
188. Keynes J. M. The General Theory of Employment, Interest and Money, London, I936. 139 p.
189. Kniazieva O., Obodovskyi Y. The infuence of the informal component on the transformation processes of the enterprise management structures. *Tree Seas Economic Journal*, Volume 1 Number 1. Riga: Publishing House "Baltija Publishing", 2020, P. 1-6.
190. Marshall Alfred *Principles of Economics*. Prometheus; Revised edition, 1997. 320 p.
191. Merriam-Webster's Collegiate Dictionary. 2003. Merriam-Webster, 1664 p. URL: http://www.merriam webster.com/netdict/anticipation
192. Ross S. A. *Compensation, Incentives, and the Duality of Risk Aversion and Riskiness.* Journal of Finance. Vol. 59. 2004. Pp. 207–225.
193. Shvydanenko G. Intellectualization of business planning process in the modern economic conditions. *Social processes regulation in the context of economics, law and management*: Materials digest of the LIII International Research and Practice Conference and II stage of the Championship in economics, management and juridical sciences, (London, June 06-June 11,

2013). International Academy of Science and Higher Education. London: IASHE, 2013. PP. 69–73.
194. Slywotzky A. Turning *Strategic Risk into Growth Opportunities*. Harvard Business Review. 2008. Sep 15. Pp. 78–88.
195. *Technology and Communications Industry Report. URL: http://www.aon.com.*
196. The Global Innovation Index (GII) 2020. Who Will Finance Innovation? *URL: https://www.globalinnovationindex.org/gii-2018-report*
197. *UN E-Government Survey 2018.* URL: https://public-l administration.un.org/egovkb/en-us/Reports/UN-EGovernment-Survey-2018?fbclid=IwAR0ROie7FQWAo7F3USIMIS5ePu2YMA40NLQ2rA52uUAUX6QCZJdtXtT2k8https://publicadministration.un.org/ egovkb/en-us/Data/Country-Information/id/180-Ukraine
198. Zakharzhevska A., Al-Ababneh Hassan Ali, Borisova V., Tkachenko P., Andrusiak N. Performance of Artificial Intelligence Technologies in Banking. WSEAS TRANSACTIONS on BUSINESS and ECONOMICS. Vol. 20, 2023, pp.307-317.
199. Zakharzhevska A., Vynogradova O., Drokina N. Directions of activation of risk management of telecommunications enterprises in Ukraine in martial law and post-war conditions. Acta Scientiarum Polonorum. Oeconomia, 28(4), 2022.
200. Zakharzhevska A., Zghurska O., Malik M., Baidala V., Somkina T., Kubiv S., Huzhavina I., Sukhostavets A., Kulik A. Modelling the influence of the environmental factor on ensuring the sustainability of Ukraine's food security. *Journal of Hygienic Engineering and Design. Vol.40, 2022, pp. 191–200.*
201. Zakharzhevska A. A. Formation of strategic guidelines for risk management in telecommunications enterprises. *Економіка. Менеджмент. Бізнес*. № 3-4 (40), 2022. С. 54–61.
202. Zakharzhevska A., Vynogradova O., Pysar N. The formation of strategic portfolio of the development of risk management in telecommunications enterprises during martial law and post-war conditions. *Technology Audit and Production Reserves, Economics of enterprises. Macroeconomics Vol.№6(4(68),2022 P.12- 16/*
203. Zakharzhevska A.A. Key factors that influence the development of risk management of telecommunications enterprises in the conditions of digitalisation of the economy. V Міжнародна науково-практична конференція „SCIENCE and INNOVATION of MODERN WORLD" 25-27.01.2023 р. (м. Лондон, Великобританія).
204. Zakharzhevska A. A. Strategic guidelines for risk management in telecommunications enterprises. *The 2nd International scientific and practical conference "Scientific progress: innovations, achievements and prospects"* (November 6-8, 2022) MDPC Publishing, Munich, Germany. 2022. 596 p. P.478-482.
205. Гудзь О.Є., Рубцов В.С. *Управління ризиками при реалізації власних бізнесових проектів (Ризик менеджмент у малому та середньому бізнесі*): Навч. Посібник. Київ. Планета людей, 2003. 88 с. с.5 – 78.
206. Гудзь О.Є. Рубцов В.С. *Мистецтво бізнесу або управління бізнесовими проектами: Навч. посібник*. Київ. Планета людей, 2006. 159 с. С.12 –159.
207. Гудзь О.Є., Глушенкова А.А. *Менеджмент ідей та управління проектами*: навч. посібник. Київ. Планета людей, 2016. 156 с.
208. Гудзь О.Є. *Інноваційне підприємництво*. Київ. Планета людей, 2018. 187 с.
209. Абакуменко О.В. Моделювання рівня конкуренції на фінансовому ринку України. *Бізнесінформ*. 2013. № 5. С. 302–310
210. Базилевич В.Д. Новітні тенденції та протиріччя на страховому ринку України. *Вісник КНУ імені Тараса Шевченка. Економіка*. 2012. Вип. 133. С. 5- 8.
211. Братюк В.П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки*. 2015/ № 9. С. 421-427
212. Вороненко Т. Безпечний Інтернет URL: http://calameo.com/books/002793881c6046eb0d2fb

213. Гаманкова О.О. Інформаційні вади дослідження ступеня монополізації ринку страхових послуг України. *Актуальні проблеми економіки*. 2009. № 10. С. 80 – 87.
214. Золотарьова О.В. Ключові тенденції та пріоритети розвитку ринку страхових послуг в Україні *Економіка і суспільство*. 2017. №11. С. 413-420.
215. Іващенко А.М. Світовий ринок страхування кібер-ризиків: перспективи та перешкоди. *Матеріали IX Міжнародної науково-практичної конференції „Національна економіка: проблеми та перспективи розвитку*. Київ КНУ, 2016. С. 196–202.
216. Кулина Г. Світовий ринок страхових послуг в умовах зміни парадигми глобального економічного розвитку. *Світ фінансів*. 2017. № 3(52). С. 48-59.
217. Малікова І.П. Оцінка концентрації страхового ринку України, її зв'язок з процесами монополізації та конкуренції. *Науковий вісник Херсонського державного університету. Серія «Економічні науки»*. 2017. Вип. 23. С. 76-79.
218. Підсумки діяльності страхових компаній за 2017 рік. URL: https://www.nfp.gov.ua/files/OgliadRinkiv/SK/2017 _rik/sk _% 202017.pdf
219. Пономарьова О.Б. Визначення проблем страхового ринку та їх вирішення. *Глобальні та національні проблеми економіки*. 2015. №5.
220. Приказюк Н.В. Прогресивний досвід зарубіжних країн у вирішенні проблем розвитку кіберстрахування. *Вісник ОНУ. Серія: «Економіка»*. 2016. Вип. 2. С. 164-168.
221. Allianz Risk Barometer Top Business Risks 2016. Available at: http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf
222. Böhme R., Schwartz G. (2010) Modeling cyber-insurance: towards a unifying framework. WEIS. Available at: http://econinfosec.org/ archive/weis2010/papers/session5/weis.
223. Marotta A. A Survey on Cyber-Insurance. Marotta A., Martinelli F., Nanni S., Yautsiukhin A. Bologna, Italy: Unipol Gruppo Finanziario S.p.A. (in English)
224. The digital insurer. A new era in insurance: Cloud computing changes the game.
225. World insurance in 2015: steady growth amid regional disparities. Available at: http://media.swissre.com/documents/sigma_3_2016_en.pdf.
226. 1ANSI PMI PMBOK® Guide 3rd Edition. URL: http://webstore.ansi.org/.
227. Glossary of Project Management Terms. URL: http://www.uc.edu/sashtml/ orpm/chapa/index.htm.
228. SimonBuehring Управління невеликими проектами. URL: Simon Buehring. http://www.pmtoday/project-management/role/managing-small-projects
229. Батенко Л. П.Управління проектами. Київ. КНЕУ, 2005. 231 с.
230. Dennis Lock *Project management* (9e ed.) Gower Publishing, Ltd., 2007.
231. Richard E. Just, Darrell L. Hueth, Andrew Schmitz. The Welfare Economics of Public Policy: A Practical Approach to Project And Policy Evaluation, Edward Elgar Pub. 2004. 712 p.
232. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р.
233. Будзан Б. *Менеджмент в Україні: сучасність і перспективи*. Київ. Основи, 2001. 349 с.
234. Гален Грумен. URL: https://www.infoworld.com/article/3080644/it-management/what-digital-transformation-really-means.html
235. Гончаренко О.М. *Методологічні засади розробки нової редакції Концепції Національної безпеки України*. Київ. Нац. ін-т стратег, досл., 2001. 154 с.
236. *Економічний словник – довідник*. За ред. С.В.Мочерного. Київ. Femina, 1995. 430 с.
237. Єрохін С.А. Основні засади формування стратегій соціально-економічного розвитку України. *Актуальні проблеми економіки*. 2004. № 12. С.17 − 23.
238. Зуб А.Т. *Стратегічний менеджмент*. Київ Знання. 2001. 315 с.
239. Котлер Ф. *Основи маркетингу*. Київ. КПІ, 1994. 675 с.
240. Кредісов А. Стратегічний менеджмент на початку XXI ст.: зміна парадигми. *Економіка України*. 2011. № 2. С. 28-37.

241. Манов В. *Реформи в постсоціалістичній державі: досвід Болгарії*. Київ КНЕУ, 2000. 234 с.
242. Минцберг Г. *Стратегічний процес*. Київ. ЦНУ, 2001. 543 с.
243. Почепцов Г. Стратегія як мистецтво і особливий вид політики. *Політичний менеджмент*. 2004. № 2. с. 250.
244. *Довідник іншомовних слів*. Київ, 1964. 675 с.
245. Соловей В.С. *Стратегічний менеджмент*. Київ НАУ, 2002. 342 с.
246. *Стратегічний менеджмент* за ред. Д.Кэмпбел, Дж.Стоунхаус, Б.Хьюстон. Харків. ХНДУ. 2003. 336 с.
247. Шубін О. Стратегічне управління як основна частина системи менеджменту підприємства. *Журнал європейської економіки*. 2003. №4. 76 с
248. Chandler A. *Strategy and Structure*: Chapters in the History of the American Industrial Enterprise, MA: MIT Press, 1962.-466 p.
249. *Digital transformation: the essentials of e-business leadership*, by Keyur Patel, Mary Pat McCarthy, 2000.
250. *Digital Transformation* By Mark Baker, 2014,
251. URL: https://en.oxforddictionaries.com/definition/digital
252. URL: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-europe-realizing-the-continents-potential
253. *Knowledge exchange partnership leads to digital transformation* at Hydro-X Water Treatment, Ltd. Global Business and Organizational Excellence. 2018; 37:6–13, by Heinze A, Gri ths M, Fenton A, Fletcher G.
254. Lankshear, Colin; Knobel, Michele (2008). *Digital literacies: concepts, policies and practices*. p. 173.
255. Polak B. ECON 159: Game Theory. Lecture 1 Transcript. Open Yale Courses. 5 September 2007. URL: http://oyc.yale.edu/economics/econ-159.
256. Rowe A. *Strategic Management*. Dickel K. -N.Y., 1996.-953 p.
257. Stolterman, Erik; Croon Fors, Anna (2004). *Information Technology and the Good Life*". Information systems research: relevant theory and informed practice. p. 689.
258. Thompson J.L. *Strategic Management*: Awareness and Change. Cengage Learning EMEA, 2001. 1141 p.

ДОДАТКИ

Додаток А

Еволюція категорії „ризик”

Період	Школа, течія економічної науки	Вклад у розвиток теорії економічного ризику
XII-XIV ст.	Теорія відсотка	Каноністи (церковне вчення): відсоток за кредит − плата за ризик.
XVI ст.	−	Епоха середньовіччя (сфера мореплавства та морської торгівлі): позначення проблемних питань у різних сферах суспільного життя, окреслення яких не могло бути чітко здійснене за допомогою визначень.
XVII ст.	−	Російська імперія: перше тлумачення терміну „ризик” та опублікування його в тлумачному словнику (В. І. Даль та С І. Ожегов): „ризик” − можливість небезпеки.
Початок XVIII ст.	Класична економічна теорія	Фома Аквінський: ризик − це втрата позичених грошей, тобто певна негативна дія, котра може настати, якщо позикові кошти будуть втрачені. Адам Сміт: „ризик” − чинник формування частини ирибугку, як плата за управлінські здібності капіталіста.
Друга половина XVIII ст.	Школа фізіократів	Жак Тюрго: прибуток − це заробітна плата за ризик. Становлення підприємця як людини, що ризикує своїм капіталом, землею та ін. для отримання підприємницького доходу.
Кінець XVIII ст.	Класична теорія ризику	Ризик − збиток завданий здійсненням обраного рішення. Ризик − ймовірність отримання збитків.
Початок XIX ст.	Марксистська теорія	Карл Маркс: ризик − це страх втрати чи псування цінних матеріалів чи робочої сили.
Друга половина XIX ст.	Неокласична школа	Ральфа Джорджа Хоутрі: ризик − це певна сукупність здібностей підприємця чи торговця, при виробництві та реалізації товарів.
Середина XIX ст.	Кепсіанська терія ризику	Дж. Кейнс: ризик − чинник задоволення, який полягає в очікуванні великого прибутку.
Кінець XIX ст.	Неолібералізм	Ризик стає вирішальним чинником формування прибутку.
Початок XX ст.	Інституціоналізм, інноваційна теорія	Інновація виступає як компенсація ризику.
Кінець XX ст.	Сучасна теорія ризику	Ризик − це небезпека потенційно можливої, ймовірної втрати ресурсів або недоотримання доходів у порівнянні з варіантом, який розрахований на раціональне використання ресурсів у конкретній бізнесовій діяльності.
Початок XXI ст.	Інформаційна теорія ризику	Ризик − це загрози, які можуть негативно вплинути на безпеку інформаційної системи та вивести її з ладу в цілому.

Додаток Б

Змістове наповнення трактування різними дослідниками поняття „ризик”

Визначення	Джерело
Термін „ризик” передбачає будь-яку події або дію, що можуть негативно позначитися па досягненні підприємством її намічених цілей і завадити йому успішно реалізувати свою стратегію.	А. Андерсен
Під ризиком розуміється можлива небезпека втрат, що витікає зі специфіки тих чи інших явищ природи та видів діяльності людського суспільства.	І. Т. Балабанов
Ризик ситуація, коли мають місце невизначеність, конфлікт, наявна багатоваріантність, і коли одночасно не всі альтернативні варіанти і є складовим елементом будь-якої управлінської діяльності.	В. В. Вітлінський, Г Великоіваннсько
Ризик − це можливість події, неочікуваної для активного суб’єкту, яка може виникнути в період переходу суб’єкта із даної початкової ситуації до заздалегідь визначеною цим суб’єктом кінцевої ситуації.	В. Н. Вяткін, І. Вяткін
Ризик діяльність, пов’язана з подоланням невизначеності в ситуації неминучого вибору, у процесі якого є можливість якісно і кількісно оцінити ймовірність досягнення передбаченого результату, невдачі, відхилення від мети.	Л. І. Донець
Ризик − це єдність обставин та індивідуально-групових критеріїв оцінки ситуації, на основі яких приймається оперативне рішення.	Загальнонауков е значення
Ризик − це усвідомлення можливості небезпеки виникнення непередбачених втрат очікуваного прибутку, майна, грошей у зв’язку з випадковими змінами умов економічної діяльності, несприятливими обставинами.	А. Г. Загородній, Г. Л. Вознюк
Ризик − це можливість відхилення від передбачуваної мети, заради якої здійснюється вибрана альтернатива.	І. Ю. Івченко
Ризик у загальному випадку слід розглядати як можливість або загрозу відхилення результатів конкретних рішень або дій від очікуваних.	С. М Ілляшенко
Ризик це ймовірність виникнення страт, недоотримання прибутків, небажаного розвитку середовища функціонування, відхилення від установлених цілей.	О. Є. Кузьмін, О. Мельник
Ризик − це ситуація невизначеності, неоднозначності, яка може призвести як до позитивного, так і до негативного результату того чи іншого економічного дії.	М. Г. Лапуста, Л. Шаршукова
Ризик − це об’єктивно-суб’єктивна категорія, пов’язана з подоланням невизначеності, випадковості, конфліктності в ситуації неминучого вибору, що відображає ступінь досягнення суб’єктом очікуваного результату.	В. Лук'янова, Т. Головач
Ризик − імовірність втрати підприємством частини своїх ресурсів, недоодержання доходів чи появи додаткових витрат у результаті здійснення певної виробничої і фінансової діяльності	Н. І. Машина
Ризик − це можливість виникнення неблагополучних ситуацій в ході реалізації планів і виконання бюджетів підприємства.	Л. Н. Тепман
Ризик в економічному розумінні передбачає втрати, ймовірність котрих пов’язана з наявністю невизначеності, а також зиск і прибуток, отримати які можливо завдяки діям, пов’язаним з ризиком.	А. В. Шегда, О. Голованенко

Додаток В

Сучасні моделі та концепції економічного розвитку [*56, 124, 125, 170*]

Назва моделі	Характеристика
Моделі економічного розвитку	
Модель лінійних стадій розвитку	будь-яка економічна система в процесі свого розвитку має пройти певні етапи, за умови включення її в світову систему взаємозв'язків.
Теорія структурних трансформацій	відображає процес переходу від аграрної до індустріальної моделі економічного розвитку
Теорія зовнішньої залежності	взаємозалежність країн світу є наслідком залежності колоній від метрополій та інших розвинутих країн. Тому між ними сформовані відносини нееквівалентного обміну у взаємній торгівлі.
Неокласична модель вільного ринку	необхідність лібералізації економіки, її зовнішньої відкритості, приватизації власності, інституційної перебудови тощо
Теорія ендогенного зростання	орієнтації на внутрішні чинники і механізми господарського розвитку.
Модель сталого розвитку	спрямована на зміну стосунків людини і природи задля розширення можливостей економічного зростання, та на створення скоординованої глобальної стратегії виживання людства, орієнтованої на збереження і відновлення природних спільнот.
Концепція життєвих циклів А.Адізеса	в ефективній організації повинні бути представлені усі чотири управлінські функції: Р – орієнтована на результати, А - адміністративна, Е – підприємницька і І – інтеграційна. Отже, підприємство повинно оптимальним чином задовольняти споживачів, вчасно змінюватись та попереджувати потреби, що змінюються, створивши для цього структуру з взаємозамінних елементів
Концепція еволюційного розвитку підприємства Л.Грейнера	На кожній стадії діяльність підприємства фокусується на якомусь конкретному аспекті, і кожна стадія завершується кризою, що несе загрозу виживанню підприємства. Якщо підприємство справляється з кризою успішно, то воно вступає в наступну стадію

Додаток Д

Переваги та недоліки використання наукових підходів в управлінні економічним розвитком підприємства [*56, 124, 125, 170*]

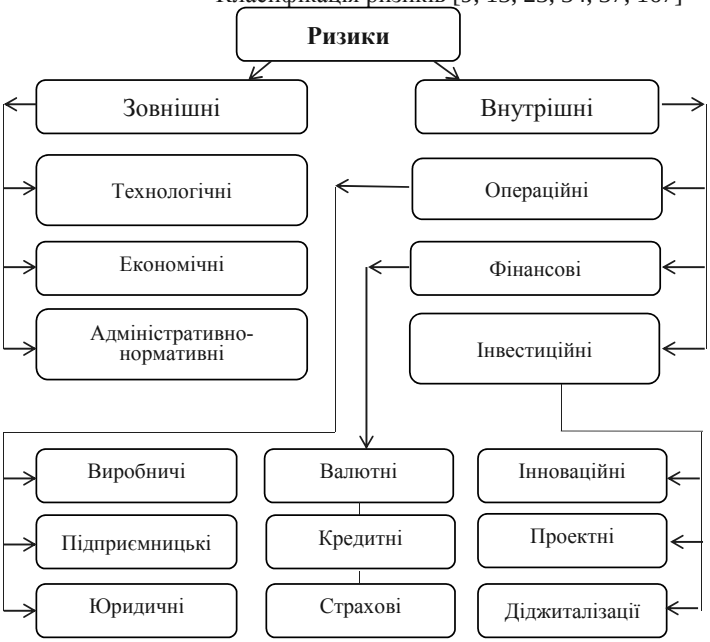
Назва підходу	Переваги підходу	Недоліки підходу
Системний підхід	Визначення цілей та критеріїв управління та підпорядкування встановлених критеріїв загальній меті; Розгляд усіх елементів системи у взаємозв'язку; Застосування на різних рівнях — від одного підрозділу до всього підприємства. У кожному випадку об'єкт управління розглядається як цілісна система; Спрямування на слабо структуровані проблеми, пошук оптимального варіанта їх вирішення	Потребує високого професіоналізму персоналу; Використання дорогих технологій, автоматизованих систем управління; - Не передбачає розкладання на взаємопов'язані процедури як на «вході» з постачальниками, так і на «виході» з покупцями і замовниками
Програмно-цільовий підхід	Робить більш зрозумілою організаційну структуру управління організацією; Забезпечує цілеспрямовану мотивацію робітників; Допомагає опрацювати ефективні методи контролю (винагороджується результат, а не процес діяльності). Найкращим орієнтиром для контролю є комплекс чітко сформульованих цілей.	Керівникам іноді важко встановлювати кількісно визначені цілі діяльності для кожного підлеглого. Вищим керівникам не завжди вигідно доводити цілі до кожного підлеглого. Потребує встановлення короткострокових цілей; значної бюрократії; високої кваліфікації персоналу.
Ситуаційний підхід	Досягнення мети підприємства в даних умовах часу; Визначення умов формування концепції підприємства щодо розвитку системи управління; Врахування конкретного набору обставин, що впливають на підприємство у визначений проміжок часу; Знаходження оптимальних рішень у конкретних ситуаціях; Суттєва економія часу, коли потрібно оперативно прийняти рішення	Орієнтація виключно на стандартні завдання; Відсутність стратегічного планування; Складність формування критеріїв оцінки ефективності управління враховуючи широкий спектр ситуацій, що виникають на підприємстві, у зв'язку з чим звужується керованість управлінського процесу; Управління виконується на рівні ситуації, коли вона керує процесом, а не процес ситуацією.

Продовження додатку Д

1	2	3
Функціональний підхід	Управління здійснюється сукупністю підрозділів, що спеціалізуються на виконанні конкретного виду робіт; Високий рівень професіоналізму працівників; Отримання механізму найшвидшої реакції на зміни умов господарювання; чіткий розподіл функцій дає можливість забезпечити стійкий розвиток підприємства; Зростання якості управління основною діяльністю	Обмежені зони відповідальності; Надмірний рівень бюрократії (погоджень, контролю, делегування повноважень і т.д.); Працівники зосереджені на процесі виконання роботи, а не на кінцевому результаті; Велика кількість узгоджень, що збільшує термін виконання роботи до одержання кінцевого результату
Процесний підхід	Високий рівень якості управління; Мінімізація функцій, що контролюються; Оптимізація централізованого та децентралізованого підходів; Зниження ризику субоптимізації при управлінні цілісним процесом; Відхід від фрагментарної відповідальності; Управління процесами дозволяє створити кращі підстави для контролю ресурсів і часу виконання робіт; Урахування динамічного характеру розвитку організацій; Істотне скорочення витрат на управління	Високий рівень фінансування при переході на управління за процесним підходом; Труднощі сприйняття працівниками нового підходу до управління; Складність реалізації підходу; Недостатність відображення взаємозв'язку між елементами управління; Зниження можливості професійного зростання та звуження компетенції робітників

Додаток Е

Класифікація ризиків [9, 13, 23, 34, 37, 167]



Продовження додатку Е. Ризики проекту [98, 99 с. 723]

Додаток К

Загальні принципи управління на підприємстві
(систематизовано авторами на основі [144 с.25-27])

Принцип управління	Характеристика принципу управління
Принцип наукової обґрунтованості управління	Цей принцип – основний в системі загальних принципів управління. Науковий підхід до менеджменту вимагає комплексного вивчення всієї сукупності чинників, що впливають на ефективність функціонування організації, з подальшим застосуванням отриманих знань у практиці управління
Принцип системного підходу до вирішення управлінських завдань	Системний підхід вимагає, щоб керівники розглядали організацію як сукупність взаємопов'язаних, взаємозалежних і постійно взаємодіють один з одним елементів (люди, структура; завдання і технології), орієнтованих на досягнення різних цілей
Принцип оптимальності управління	Принцип оптимальності управління встановлює вимогу досягнення цілей управління з мінімальними витратами часу і коштів
Принцип гнучкості управління	З вищеназваним принципом нерозривно пов'язаний принцип гнучкості управління, практична реалізація якого дозволяє забезпечити своєчасну адаптацію організації до мінливих умов зовнішнього середовища або її швидку перебудову відповідно до новими цілями функціонування
Принцип демократизації управління	Із зростанням ролі соціальних чинників в менеджменті на перший план вийшов принцип демократизації управління, який містить вимогу задоволення на справедливій основі інтересів власників, керівників, трудового колективу і окремих працівників організації
Принцип регламентації управління	Відповідно до принципу регламентації всі процеси, що відбуваються в системі управління, повинні бути жорстко регламентовані, тобто в будь-якій організації повинна бути розроблена розгорнута система правил і норм, що визначають порядок функціонування як організації в цілому, так і її окремих структурних підрозділів
Принцип формалізації управління	Принцип формалізації передбачає формальне закріплення норм і правил функціонування організації у вигляді наказів, вказівок і розпоряджень керівника, а також у вигляді положень про конкретні структурні підрозділи та посадових інструкцій

Додаток Л

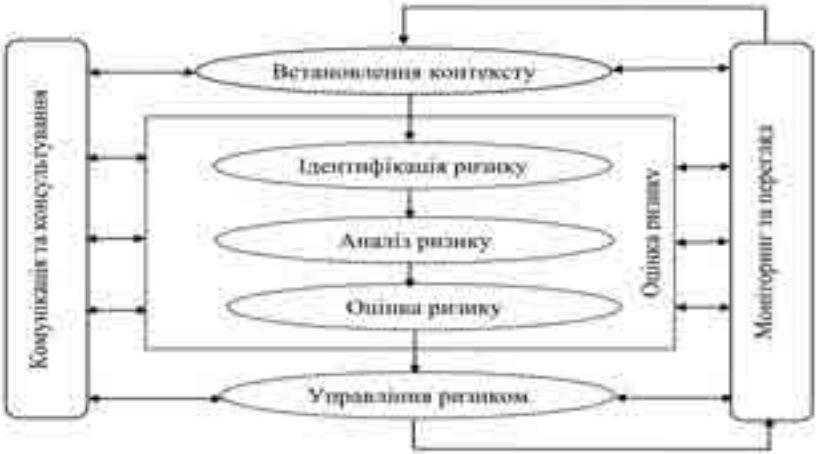
Принципи управління ризиками в наукових працях
(систематизовано авторами)

Автори	Рік	Назва праці	Принципи згідно із стандартом
Караєва Н.В., Войтко С.В., Сорокіна Л.В. [86 с.60]	2013	Ризик-менеджмент сталого розвитку енергетики: інформаційна підтримка прийняття рішень	1) принцип масштабності; 2) прагнення до врахування якомога більшої кількості сфер можливого виникнення ризиків; 3) принцип мінімізації; 4) необхідність зменшення спектра проявів ризиків і ступеня їх впливу; 5) принцип адекватності реакції; 6) необхідність швидко і ефективно реагувати на зовнішні зміни в ризикованій ситуації; 7) принцип розумного прийняття; 8) прийняття ризику тільки у випадку його обгрунтованої необхідності.
Семенова К.Д., Тарасова К.І. [146 с.46-47]	2017	Ризики діяльності промислових підприємств: інтегральне оцінювання	1) принцип максимальності виграшу, який полягає в тому, що з можливих варіантів ризикових вкладень капіталу обирається той, який дає найбільшу ефективність результату при мінімальному чи прийнятному для підприємства рівні ризику; 2) принцип оптимальної ймовірності результату, який стверджує, що з усієї сукупності можливих рішень обирають те, при якому вірогідність результату є прийнятною для підприємства; 3) принцип оптимального сполучення виграшу та величини ризику, згідно якого з усіх варіантів, що забезпечують прийнятний для підприємства ризик, обирається той, у якого співвідношення прибутку до втрат (збитку) є найбільшим; 4) принцип оптимального коливання результату полягає в тому, що з можливих рішень обирається те, при якому ймовірності виграшу чи програшу для самого ризикового проекту мають найменший розрив; 5) принцип мінімізації спектру можливих ризиків і ступеня їх впливу на діяльність господарюючого суб'єкта; 6) принцип адекватності реакції, який зводиться до того, що необхідно адекватно та швидко реагувати на зміни, які можуть призвести до виникнення ризику; 7) принцип прийняття – підприємство може прийняти на себе лише обгрунтований ризик
Коваленко В.В. [147 с.17]	2017	Система ризик-менеджменту в банках: теоретичні та методологічні аспекти	1) ефективність; 2) своєчасність; 3) структурованість; 4) розподіл обов'язків (відокремлення функції контролю від здійснення операцій банку); 5) усебічність та комплексність; 6) пропорційність;

			7) незалежність; 8) конфіденційність; 9) прозорість
Боровик М.В. [14 с.27]	2018	Ризик-менеджмент	1) принцип лояльного ставлення до ризиків; 2) принцип прогнозування; 3) принцип страхування; 4) принцип резервування; 5) принцип мінімізації втрат і максимізації доходів
Мороз В.М., Мороз С.А. [112 с.63]	2018	Ризик-менеджмент	1) системність та безперервність дій щодо виявлення та оцінювання ризиків; 2) персональна відповідальність суб'єктів управління за якість ризик-менеджменту на рівні структурного підрозділу; 3) комплексне сприйняття впливу ризиків в процесі прийняття управлінських рішень; 4) аналіз рівня прояву ризиків на всіх етапах управлінської діяльності; 5) обов'язковість дотримання регламенту внутрішнього та зовнішнього контролю процедур ризик-менеджменту; 6) оцінювання ефективності ризик-менеджменту; 7) колегіальність в обговоренні та прийнятті рішень
Герасименко О.М. [27 с.166-168]	2021	Ризик-орієнтоване управління в системі економічної безпеки підприємства	1) інтегрованість; 2) структурованість та комплексність; 3) адаптованість; 4) інклюзивність; 5) динамічність; 6) надійність інформації; 7) людський та культурний чинники; 8) постійне вдосконалення.

Додаток Х

Процес управління ризиками згідно ISO 31000:2018 [53]



Додаток М

Порівняльна характеристика основних теоретичних концепцій управління ризиками підприємств [9, 13, 23, 34, 37, 167]

Назва концепції			
Основні характеристики	Інтуїтивна	Фрагментарна	Комплексна (ERM)
Мета управління	Уникнення ризиків	Захист від негативного впливу ризиків	Використання висхідних можливостей створюваних невизначеністю
Ризики, що підлягають розгляду	Мінімальна кількість ризиків	Обмежена кількість ризиків	Всі ризики підприємства
Підхід до управління	Хаотичний (розгляд окремих ризиків)	Дезінгегрований підхід (окремий розгляд ризиків)	Комплексний підхід (портфель ризиків)
Аспекти управління	Фінансові наслідки	Фінансові наслідки	Стратегічні можливості та наслідки, що проходять через всі функції фірми
Процес управління	Орієнтований на захист	Орієнтований на продукт	Орієнтований на процес ідентифікації характеристики ризику
Характер взаємодії	Реактивний	Реактивний	Проактивний
Результат управління	Повне або часткове уникнення ризику	Зниження волатильності прибутку, виручки, грошових потоків або вартості фірми.	Зростання вартості фірми в коротко- і довгостроковій перспективі.
Вплив на діяльність підприємства	Мінімальний вплив	Обмежений вплив на стратегії	Підтримка стратегічного і бізнес-планування
Основні методи управління	Відмова / страхування	Страхування	Використання переваг високої волатильності

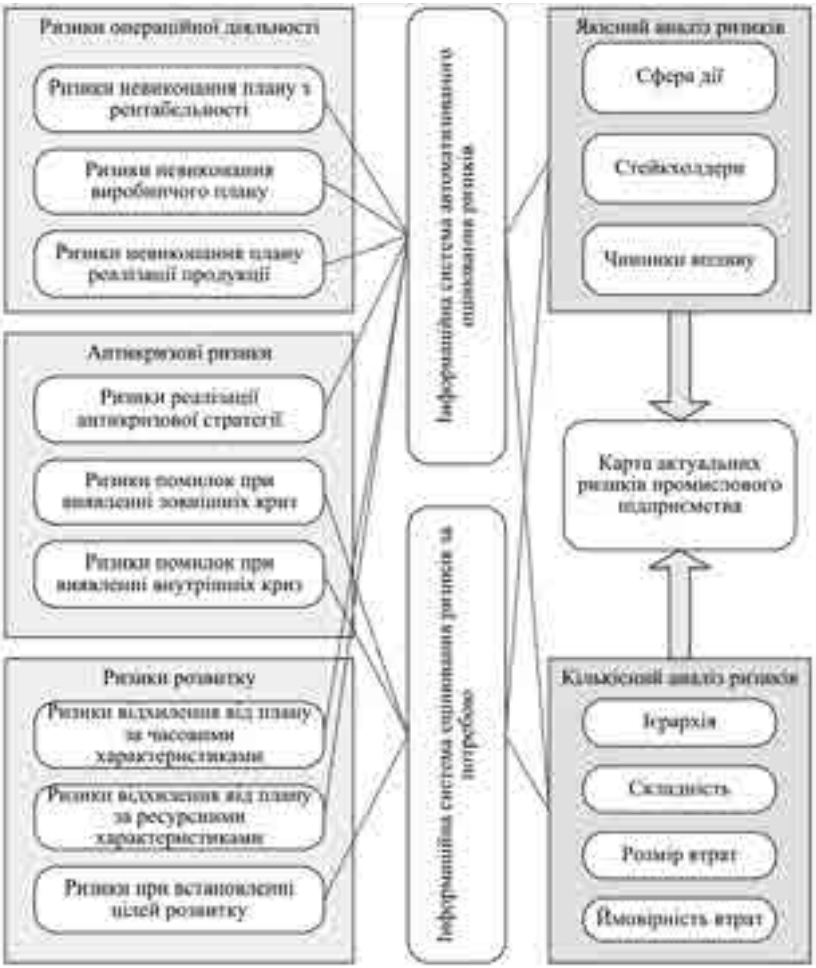
Додаток Н

Модель COSO ERM [119]

Додаток П. Чинники ризику згідно FERMA RMS [53]

Додаток Р

Система оцінювання ризиків підприємства [*5, 34, 91, 99, 101, 154, 160*]



Додаток С. Комплексна оцінка ризиків підприємства та прийняття управлінських рішень на основі результатів оцінки [*5, 34, 91, 98, 99, 101, 154, 160*]

Додаток Т

Обґрунтування системи показників для визначення рівня економічної стійкості підприємства з урахуванням структурованих чинників ризику *(авторська розробка)*

Показник	Алгоритм розрахунку	Умовне позначення	Логіка обґрунтування цільових та граничних значень
1	2	3	4
1. Показники, що характеризують економічну стійкість підприємства з позицій фінансово-економічних чинників ризиків			
1.1. Коефіцієнт поточної ліквідності	$К_{пл} = \frac{ОА}{ПЗ}$, де *ОА* – оборотні активи *ПЗ* – поточні зобов'язання	$К_{пл}$	Залежить від обраних політик формування та фінансування оборотних активів
1.2. Коефіцієнт швидкої ліквідності	$К_{шл} = \frac{ДЗ + ГК}{ПЗ}$, де *ДЗ* – дебіторська заборгованість *ГК* – грошові кошти	$К_{шл}$	Залежить від обраної політики формування оборотних активів
1.3. Коефіцієнт негайної ліквідності	$К_{нл} = \frac{ГК}{ПЗ}$,	$К_{нл}$	Залежить від обраної політики формування оборотних активів
1.4. Середньозважений період обертання оборотних активів	$Клоа =$ $Ч_{з} * ПО_{з} + Ч_{дз} * ПО_{дз} + Ч_{гк} * ПО_{гк}$	$К_{лоа}$	Залежить від структури оборотних активів та обраної політики
1.5. Коефіцієнт автономії	$К_{фа} = \frac{ВК}{ЗК}$ де *ВК* – власний капітал *ЗК* – загальний обсяг задіяного капіталу	$К_{фа}$	Залежить від політики формування капіталу
1.6. Коефіцієнт маневреності капіталу	$К_{мк} = \frac{ВОК}{ВК}$ де *ВОК* – власний оборотний капітал	$К_{мк}$	Залежить від обраної політики фінансування оборотних активів
1.7. Коефіцієнт збалансованості поточних зобов'язань	$К_{зз} = \frac{КЗ}{ДЗ}$ де *КЗ* – кредиторська заборгованість	$К_{зз}$	Співвідношення непрострочених кредиторської і дебіторської заборгованостей має бути 1-1,5
1.8. Коефіцієнт синхронності грошових потоків	$К_{сгп} = \frac{\sqrt{\sum_{t=1}^{m} \frac{(N_t - V_t)}{n}}}{V}$ де N_t - надходження грошових коштів за *t*період	$К_{сгп}$	Вхідні та вихідні потоки повинні бути збалансованими, тому оптимальне значення має

	V_t - витрачання грошових коштів за *t*період *n*– кількість досліджуваних періодів V - загальний обсяг вихідного грошового потоку		наближуватись до 0
1.9. Коефіцієнт кратності відсотків	$$К_{кв} = \frac{П_{до} + В_{фін} + АМ}{В_{фін}}$$ де $П_{до}$ - прибуток від звичайної діяльності до оподаткування $В_{фін}$ - фінансові витрати *АМ* – амортизаційні витрати	$К_{кв}$	Максимізація даного коефіцієнту свідчить про зниження фінансових ризиків
1.10 Індекс стабільності фінансових результатів	Середньоквадратичне відхилення фінансових результатів (прибутку) протягом досліджуваного періоду / середній обсяг фінансового результату	$I_{сп}$	Мінімізація даного коефіцієнту свідчить про зниження ризиків
2. Показники, що характеризують економічну стійкість підприємства з позицій цифровізаційних чинників ризиків			
2.1. Коефіцієнт цифровізації адміністратив-них і повторюваних бізнес-операцій (у загальній системі бізнес-процесів підприємства)	$$К_{цап} = \frac{АП_{циф}}{АП_{заг}}$$ де $АП_{циф}$ - кількість адміністративних і повторюваних бізнес-операцій, у які запроваджені механізми цифровізації $АП_{заг}$ - загальна кількість адміністративних і повторюваних бізнес-операцій	$К_{цап}$	Чим вищим є значення показника тим вищим є загальний рівень цифровізації бізнес-процесів на оперативному рівні
2.2. Коефіцієнт цифрової трансформації підприємства	$$К_{цтр} = \frac{ЕО_{циф}}{ЕО_{заг}}$$ де $ЕО_{циф}$ - кількість бізнес-процесів, які здійснюються з використанням інтегрованих цифрових технологій $ЕО_{заг}$ - загальна кількість бізнес-процесів	$К_{тр}$	Чим вищим є значення показника тим вищим є загальний рівень цифровізації бізнес-процесів на стратегічному рівні
2.3. Коефіцієнт інноваційного розвитку	$$К_{інр} = \frac{Зін}{Ззаг}$$ де $Зін$ - кількість інноваційних технологічних змін, впроваджених у діяльність *Ззаг* – загальна кількість технологічних змін	$К_{інр}$	Наближення даного коефіцієнта до 1 свідчить про найбільш високий рівень інноваційної активності
2.4. Коефіцієнт прогресивності технологій надання	$$К_{ПТ} = k_в^{отех} * \frac{У_{во}}{У_о} + k_в^{стех} * \frac{У_{вс}}{У_с}$$	$К_{ПТ}$	Максимізація даного коефіцієнту свідчить про високий рівень

телекомуні-каційних послуг	де $k_в^{отех}$, $k_в^{стех}$ - коефіцієнт вагомості використання високотехнологічного обладнання в основних та супроводжуючих бізнес-процесах процесах відповідно $У_{во}$, $У_{вс}$ - вартість високотехнологічного обладнання основних та супроводжуючих технологічних процесів відповідно $У_о$, $У_с$ - загальна вартість обладнання основних та супроводжуючих технологічних процесів відповідно		застосування провідних технологій в процесі надання телекомунікацій-них послуг підприємствами
2.5. Коефіцієнт модернізації технологій	$K_{МТ} = k_в^о * \frac{У_{МО}}{У_о} + k_в^с * \frac{У_{МС}}{У_с}$ де $k_в^о$, $k_в^с$ - коефіцієнт вагомості використання обладнання в основних та супроводжуючих технологічних процесах відповідно $У_{МО}$, $У_{МС}$ - вартість модернізованого обладнання основних та супроводжуючих технологічних процесів відповідно $У_о$, $У_с$ - загальна вартість обладнання основних та супроводжуючих технологічних процесів відповідно	$K_{МТ}$	Максимізація даного коефіцієнту свідчить про достатній рівень застосування сучасних технологій у діяльності підприємства
3. Показники, що характеризують економічну стійкість підприємства з позицій інтелектуалізаційних чинників ризиків			
3.1. Коефіцієнт відповідності організаційної культури організаційній структурі підпри-ємства	$K_{ВСК} = (\frac{K_{НСТР}}{K_{СТР}}) / (\frac{K_{НКУЛ}}{K_{КУЛ}})$ де $K_{НСТР}$ - кількість належних жорстких (гнучких) елементів, що відповідають типології організаційної структури $K_{СТР}$ - загальна кількість ключових елементів організаційної структури $K_{НКУЛ}$ - кількість належних жорстких (гнучких) елементів, що відповідають типології організаційної культури $K_{КУЛ}$ - загальна кількість ключових елементів організаційної культури	$K_{ВСК}$	Наближення коефіцієнта до 1 свідчить про достатню відповідність структури культурі. Якщо $K_{ВСК} \rangle 1$ - більшого удосконалення потребує культура; якщо $K_{ВСК} \langle 1$ - реформації потребує структура
3.2. Рівень розвитку культури	$K_{РКЗ} = \frac{Ч_В + Ч_К + Ч_с}{Ч_{заг}}$	$K_{РКЗ}$	Наближення даного коефіцієнту до 1

інтелекто-орієнтованості на підприємстві	де $Ч_{В}$ - кількість співвласників, ініціюючих та підтримуючих інтелектоорієнованість $Ч_{К}$ - кількість штатних працівників, що координують процес інтелектуалізації $Ч_{С}$ - кількість штатних фахівців, задіяних у інтелектуалізацію $Ч_{заг}$ - загальна середньооблікова кількість працівників		свідчить про високий рівень розвитку культури інноваційних змін на підприємстві
3.3. Рівень заохочення працівників до підвищення рівня інтеллектуа-лізації	$$К_{ЗПЗ} = \frac{УЧ_{МЗ} + УЧ_{КП}}{УЧ_{ЗАГ}}$$ де $УЧ_{МЗ}$ - кількість працівників-, які отримали матеріальне заохочення після підвищення професійних і цифрових компетенцій $УЧ_{КП}$ - кількість працівників, які отримали кар'єрне просування після підвищення професійних і цифрових компетенцій $УЧ_{ЗАГ}$ - загальна кількість працівників підприємства	$К_{ЗПЗ}$	Наближення даного коефіцієнту до 1 свідчить про високий рівень заохочення працівників до підвищення рівня інтеллектуа-лізації
4. Показники, що характеризують економічну стійкість підприємства з позицій ринкових чинників ризиків			
4.1. Рівень споживчої прихильності	$$К_{СПП} = \frac{Ч_{ПЗАК}}{Ч_{ЗАГЗ}}$$ Де $Ч_{ПЗАК}$ - кількість споживачів, які робили повторні придбання ТК послуг $Ч_{ЗАГЗ}$ - кількість споживачів, які робили одноразові придбання послуг	$К_{СПП}$	Наближення даного коефі-цієнту до 1 свідчить про високу прихильність споживачів
4.2. Потенціал життєвого циклу телекомуніка-ційної галузі	Значення встановлюється за результатами експертної оцінки	$П_{ЖЦР}$	Наближення коефіцієнту до 1 свідчить про високий потенціал ринку
4.3.Потенціал життєвого циклу телекомунікацій-них послуг	Значення встановлюється за результатами експертної оцінки	$П_{ЖЦП}$	Наближення коефі-цієнту до 1 свідчить про високий потенціал послуг

Додаток У

Опитувальний лист виявлення основних чинників, які впливають розвиток управління ризиками підприємств у 2018-2020рр.

1. Назва телекомунікаційного підприємства

_____

2. Основний сегмент ринку

	Економ сегмент
	Масовий сегмент
	Люкс-сегмент
	Змішаний

3. Вкажіть кілька найбільш значущих, на вашу думку, чинників, що впливають на зниження кількості послуг.

Зниження рівня доходів населення (1)
Зниження ємності внутрішнього ринку (2)
Зростання інфляції (3)
Зростання цін на послуги (4)
Сезонні коливання (5)
Інше (вказати) (6)
Розподіліть чинники за рівнем їхньої значущості

4. Вкажіть можливі причини недостатнього фінансування підприємств.

Труднощі отримання банківських кредитів, внаслідок негативної кредитної історії (1)
Зменшення надходження коштів від господарських операцій через підвищення ринкових цін та скорочення обсягів реалізації (2)
Зміна структури витрат на підприємстві (3)
Зростання процентної ставки на кредит (4)
Зростання тарифів та податків (5)
Зниження прибутку (6)
Інше (вказати) (7)
Розподіліть чинники за рівнем їхньої значущості

5. Укажіть що на Вашу думку оказує вплив на умови цифровізаціїї підприємстві

Рівень розвитку IT-технологій (1)
Рівень розвитку технологічного забезпечення процесів цифровізаціїї (2)
Рівень інтелектуалізації систем управління знаннями суб'єктів господарювання (3)
Якість систем інтелектуального управління клієнтським капіталом (4)
Інше (вказати) (5)
Розподіліть чинники за рівнем їхньої значущості

6. Укажіть що на Вашу думку вплинуло на вибір обладнання Вашого підприємства

Рівень потужності і покриття (1)
Рівень впливу на навколишнє середовище (2)
Рівень високопродуктивності персональних систем (3)
Врахування всіх вимог до вхідних потоків даних (навантаження, швидкість, а також вже наявна техніка) (4)
Ємність середовища передачі даних: телефонні лінії, волоконно-оптичні кабелі, коаксіальні кабелі, бездротові та інші канали зв'язку (5)
Інше (вказати) (6)
Розподіліть чинники за рівнем їхньої значущості

7. Вкажіть можливі причини невідповідності телекомунікаційної продукції Вашого підприємства вимогам міжнародних норм стандартизації та сертифікації

Рівень відповідністю екологічним стандартам (1)
Рівень об'єднаності специфічних для галузей стандартів (2)
Рівень життєвого циклу телекомунікаційної продукції в системі екологічного управління (3)
Рівень надання послуг за встановленими показниками якості (4)
Інше (вказати) (5)
Розподіліть чинники за рівнем їхньої значущості

Навчальне видання

ГУДЗЬ Олена Євгенівна
ЗАХАРЖЕВСЬКА Аліна Анатоліївна

УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ

Навчальний посібник

Технічний редактор Лисенко В.Ф.

Формат 60х84 1/16. Ум. друк. арк 10,23. Тираж 98. Зам. 158.

Видавець і виготовлювач СПД ФО Лисенко В. Ф.
25029, м. Кропивницький, вул. Пацаєва, 14, корп. 1, кв. 101. Тел.: (0522) 322-326
Свідоцтво суб'єкта видавничої справи ДК № 3904 від 22.10.2010
E-mail: kod@kod.kr.ua